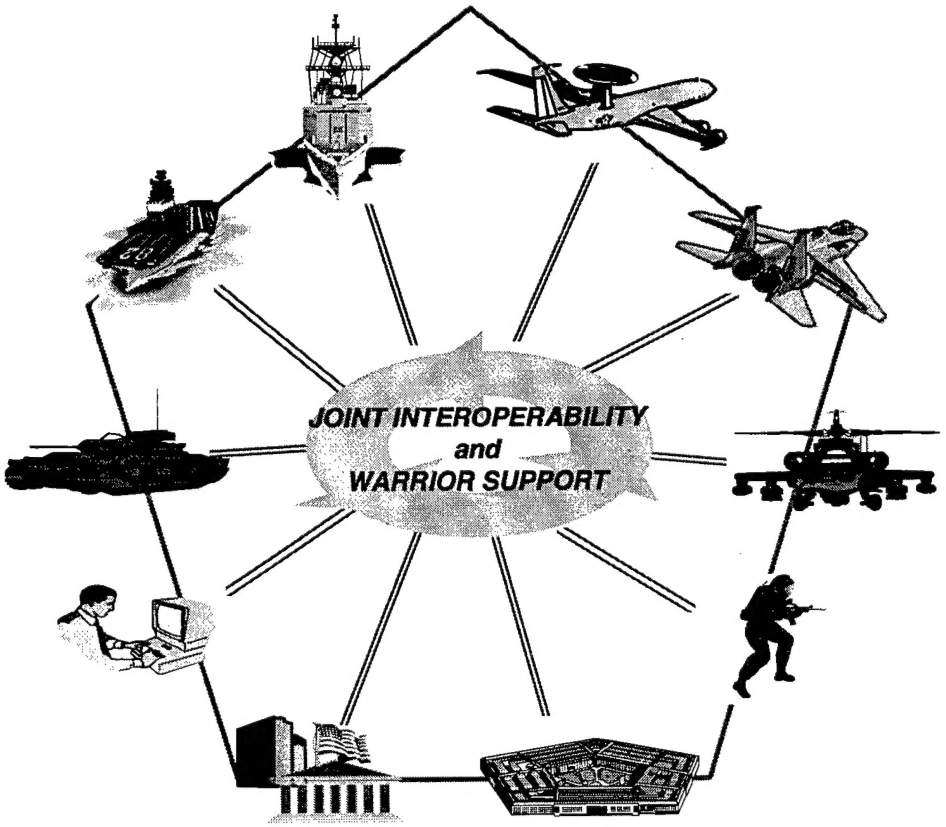
Department of Defense

Joint Technical Architecture



Version 1.0

22 August 1996

Executive Summary

The Warfighter battlespace is complex and dynamic, requiring timely and clear decisions by all levels of military command. Warfighters must be able to work together within and across Services in ways not totally defined in today's operational concepts and/or architectures. There is an unprecedented increase in the amount of data and information necessary to conduct operational planning and combat decision making. Warfighters must be able to obtain and use intelligence from theater and National assets which may be processed in forward areas or Continental United States (CONUS). Today's split base/reach back concept requires them to obtain their logistics and administrative support from both home bases and deployed locations. All of this requires that information quickly and seamlessly flow among DoD's sensors, processing and command centers and shooters to achieve dominant battlefield awareness and move inside the enemy's decision loop.

The Joint Technical Architecture (JTA) provides the "building codes" which, when implemented, permit this flow of information in support of the Warfighter. The JTA identifies a common set of mandatory information technology standards and guidelines to be used in all new and upgraded C4I acquisitions across DoD. The JTA standards are to be used for sending and receiving information (information transfer standards such as Internet Protocol suite), for understanding the information (information content and format standards such as data elements, or image interpretation standards) and for processing that information. The JTA also includes a common human-computer interface and "rules" for protecting the information (i.e., information system security standards).

The scope of this initial version of the JTA is focused on Command, Control and Intelligence systems (to include sustaining base, combat support information systems, and office automation systems) and the Communications and Computers that directly support them (C4I), and the interfaces of those systems with other key assets (e.g., weapon systems, sensors, models and simulations) to support critical joint Warfighter interoperability. Future versions of the JTA will extend the Version 1.0 scope from C4I Systems to include these other domains.

The JTA draws on the Technical Architecture Framework for Information Management (TAFIM), which provides general guidance and documents the processes and framework for defining the JTA and other technical architectures. The TAFIM applies to many DoD mission/domain areas and lists all adopted information technology standards that promote interoperability, portability, and scalability. The JTA necessarily includes requirements as related to interoperability by identifying the minimum set of standards. As the JTA evolves, the nature and relationship to the standards information in the TAFIM (particularly Volume 7) will evolve.

The standards and specifications identified in the JTA are entirely consistent with and support the DoD Standards and Acquisition Reform initiatives. The DoD standards policy recognizes the need for DoD to specify interface standards that are required for interoperability. The standards in the JTA are almost entirely performance-based interface standards. Most are commercial standards. None of the military standards require a waiver to use.

The JTA will be used by anyone involved in the management, development, or acquisition of new or improved C4I systems within DoD. Specific guidance for implementing this JTA is provided separately. While the strategy for implementation is being formulated and discussed now, the guiding principle generally agreed to is that the responsibility for specific implementation details, enforcement decisions and mechanisms will be determined by each of the Services and Agencies Acquisition Executives (SAEs). System developers will use the JTA to ensure that new and upgraded C4I systems (and the interfaces to such systems) meet interoperability requirements. System integrators will use it to facilitate the integration of existing and new systems. Operational requirements developers will be cognizant of the JTA in developing requirements and functional descriptions. When developing C4I applications for

Advanced Technology Demonstrations (ATDs), the science and technology community will use the JTA whenever possible to provide the logical interfaces to existing C4I, so that their good ideas will readily integrate into existing systems rather than require a massive redesign to meet DoD's interoperability objectives. The JTA is applicable to Advanced Concept Technology Demonstrations (ACTDs).

The JTA is a forward looking document, defining the standards to which we want to build new and upgraded systems. The intent is to clearly indicate migration direction. Legacy standards such as TADIL A, B, and C are not included. Existing systems are not expected to immediately conform to the JTA. When these systems are upgraded, the JTA will be used to transition the system towards a common interoperability goal. If legacy standards are needed to interface to existing systems they can be implemented with appropriate approval in addition to the mandated standard. Ultimately the SAEs will determine whether systems conform to the JTA, when and to what degree, based upon the business case for each acquisition.

The JTA must be a "living" document. The JTA must evolve with time as technology and the marketplace changes. In addition, it is intended that the scope of the JTA will expand to include other domains. The JTA will be jointly configuration managed by the CINCs, Services and Agencies (C/S/As). Proposed changes should be provided to the JTA point of contact identified by your CINC/Service/Agency. Changes may also be submitted via jta-comment@itsi.disa.mil. Industry and non-DoD comments should be submitted through the DISA Center for Standards (CFS) via jta-comment@itsi.disa.mil

Table of Contents

JTA SECTION 1 - OVERVIEW 1-1

1.1 INTRODUCTION 1-2
1.1.1 Purpose 1-2
1.1.2 Background 1-2
1.1.3 Architectures Defined 1-3
1.1.3.1 Operational Architecture (OA) 1-3
1.1.3.2 Systems Architecture (SA) 1-3
1.1.3.3 Technical Architecture (TA) 1-4
1.1.4 Scope 1-4
1.1.5 Applicability 1-4
1.1.6 Key Considerations in Using the JTA 1-4
1.1.7 JTA Relationship to DoD Standards Reform 1-5
1.1.8 Basis for the Joint Technical Architecture 1-5
1.1.9 JTA Relationships 1-6
1.2 DOCUMENT ORGANIZATION 1-6
1.2.1 General 1-6
1.2.2 Information Processing Standards 1-7
1.2.3 Information Transfer Standards 1-7
1.2.4 Information Modeling and Information Standards 1-7
1.2.5 Human-Computer Interfaces 1-7
1.2.6 Information Systems Security Standards 1-7
1.2.7 Appendices 1-7
1.2.8 Annexes 1-8
1.2.9 Supplements 1-8
1.3 CONFIGURATION MANAGEMENT 1-8

JTA SECTION 2 - INFORMATION PROCESSING STANDARDS 2-1

2.1 INTRODUCTION 2-1
2.1.1 Purpose 2-1
2.1.2 Scope 2-1
2.1.3 Background 2-1
2.2 MANDATES 2-2
2.2.1 Application Software Entity 2-3
2.2.2 Application Platform Entity 2-3
2.2.2.1 Service Areas 2-3
2.2.2.1.1 Software Engineering Services 2-3
2.2.2.1.2 User Interface Services 2-4
2.2.2.1.3 Data Management Services 2-4
2.2.2.1.4 Data Interchange Services 2-4
2.2.2.1.4.1 Document Interchange 2-4
2.2.2.1.4.2 Graphics Data Interchange 2-5
2.2.2.1.4.3 Geospatial Data Interchange 2-6
2.2.2.1.4.4 Imagery Data Interchange 2-6
2.2.2.1.4.5 Product Data Interchange 2-6
2.2.2.1.4.6 Audio Data Interchange 2-6
2.2.2.1.4.7 Video Data Interchange 2-7
2.2.2.1.4.8 Atmospheric Data Interchange 2-8
2.2.2.1.4.9 Oceanographic Data Interchange 2-8

2.2.2.1.4.10 Compression 2-8
2.2.2.1.5 Graphic Services 2-8
2.2.2.1.6 Communications Services 2-9
2.2.2.1.7 Operating System Services 2-9
2.2.2.2 Application Platform Cross-Area Services 2-9
2.2.2.2.1 Internationalization Services 2-9
2.2.2.2.2 Security Services 2-10
2.2.2.2.3 System Management Services 2-10
2.2.2.2.4 Distributed Computing Services 2-10
2.2.2.2.4.1 Remote Procedure Computing 2-10
2.2.2.2.4.2 Distributed Object Computing 2-10
2.3 EMERGING STANDARDS 2-11
2.3.1 Software Engineering Service 2-11
2.3.2 User Interface 2-11
2.3.3 Data Management 2-11
2.3.4 Data Interchange 2-11
2.3.5 Operating Systems 2-12

JTA SECTION 3 - INFORMATION TRANSFER STANDARDS 3-1

3.1 INTRODUCTION 3-1
3.1.1 Purpose 3-1
3.1.2 Scope 3-1
3.1.3 Background 3-1
3.2 MANDATES 3-1
3.2.1 End System Standards 3-1
3.2.1.1 Host Standards 3-2
3.2.1.1.1 Application Support Services 3-2
3.2.1.1.1.1 Electronic Mail 3-2
3.2.1.1.1.2 Directory Services 3-2
3.2.1.1.1.2.1 X.500 Directory Services 3-2
3.2.1.1.1.2.2 Domain Name System (DNS) 3-2
3.2.1.1.1.3 File Transfer 3-2
3.2.1.1.1.4 Remote Terminal 3-3
3.2.1.1.1.5 Network Management 3-3
3.2.1.1.1.6 Network Time 3-3
3.2.1.1.1.7 Bootstrap Protocol (BOOTP) 3-3
3.2.1.1.1.8 Dynamic Host Configuration Protocol (DHCP) 3-3
3.2.1.1.1.9 World Wide Web (WWW) Services 3-3
3.2.1.1.1.9.1 Hypertext Transfer Protocol (HTTP) 3-3
3.2.1.1.1.9.2 Uniform Resource Locator (URL) 3-4
3.2.1.1.1.10 Connectionless Data Transfer 3-4
3.2.1.1.2 Transport Services 3-4
3.2.1.1.2.1 Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) over Internet Protocol (IP) 3-4
3.2.1.1.2.1.1 Transmission Control Protocol (TCP) 3-4
3.2.1.1.2.1.2 User Datagram Protocol (UDP) 3-4
3.2.1.1.2.1.3 Internet Protocol (IP) 3-4
3.2.1.1.2.2 Open Systems Interconnection (OSI)/Internet Interworking Protocol 3-5
3.2.1.2 Video Teleconferencing (VTC) Standards 3-5
3.2.1.3 Facsimile Standards 3-5
3.2.1.3.1 Analog Facsimile Standard 3-5
3.2.1.3.2 Digital Facsimile Standard 3-5

3.2.1.4 Secondary Imagery Dissemination Standards 3-5
3.2.2 Network Standards 3-6
3.2.2.1 Router Standards 3-6
3.2.2.1.1 Internet Protocol (IP) 3-6
3.2.2.1.2 IP Routing 3-6
3.2.2.1.2.1 Interior Routers 3-7
3.2.2.1.2.2. Exterior Routers 3-7
3.2.2.2 Subnetworks 3-7
3.2.2.2.1 Local Area Network (LAN) Access 3-7
3.2.2.2.2 Point to Point Standards 3-7
3.2.2.2.3 Combat Net Radio (CNR) Networking 3-8
3.2.2.2.4 Integrated Services Digital Network (ISDN) 3-8
3.2.2.2.5 Asynchronous Transfer Mode (ATM) 3-9
3.2.3 Transmission Media 3-9
3.2.3.1 Military Satellite Communications (MILSATCOM) 3-9
3.2.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards 3-9
3.2.3.1.1.1 5- and 25-kHz Service 3-9
3.2.3.1.1.2 5-kHz Demand Assigned Multiple Access (DAMA) Service 3-10
3.2.3.1.1.3 25-kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service 3-10
3.2.3.1.1.4 Data Control Waveform 3-10
3.2.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards 3-10
3.2.3.1.2.1 Earth Terminals 3-10
3.2.3.1.2.2 Phase Shift Keying (PSK) Modems 3-10
3.2.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards 3-11
3.2.3.1.3.1 Low Data Rate (LDR) 3-11
3.2.3.1.3.2 Medium Data Rate (MDR) 3-11
3.2.3.2 Radio Communications 3-11
3.2.3.2.1 High Frequency (HF) 3-11
3.2.3.2.1.1 Automated Link Establishment (ALE) 3-11
3.2.3.2.1.2 Anti-jamming Capability 3-11
3.2.3.2.1.3 Data Modems 3-11
3.2.3.2.2 Very High Frequency (VHF) 3-11
3.2.3.2.3 Ultra High Frequency (UHF) 3-12
3.2.3.2.4 Super High Frequency (SHF) 3-12
3.2.3.2.5 JTIDS/MIDS Transmission Media 3-12
3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities 3-12
3.3 EMERGING STANDARDS 3-12
3.3.1 Information Transfer Standards 3-12
3.3.2 End System Standards 3-13
3.3.2.1 Internet Standards 3-13
3.3.2.2 Video Teleconferencing (VTC) Standards 3-13
3.3.2.3 Global Positioning System (GPS) 3-13
3.3.3 Network Standards 3-13
3.3.3.1 Network Access Protocols 3-13
3.3.3.2 Link 22 Transmission Standards 3-14
3.3.4 Military Satellite Communications (MILSATCOM) 3-14

JTA SECTION 4 - INFORMATION MODELING AND INFORMATION STANDARDS 4-1

4.1 INTRODUCTION 4-1
4.1.1 Purpose 4-1
4.1.2 Scope 4-1

4.1.3 Background 4-3
4.2 MANDATES 4-4
4.2.1 Activity Model 4-4
4.2.2 Data Model 4-5
4.2.3 DoD Data Definitions 4-5
4.2.4 Information Standards 4-5
4.2.4.1 Information Standards Applicability 4-5
4.2.4.2 Tactical Information Standards 4-6
4.2.4.2.1 Bit-Oriented Data 4-6
4.2.4.2.2 US Message Text Format (USMTF) Messages 4-6
4.2.4.2.3. Database-to-Database Exchange 4-7
4.3 EMERGING STANDARDS 4-7
4.3.1 Activity Model 4-7
4.3.2 Data Modeling 4-7
4.3.3 DoD Data Definitions 4-7
4.3.4 Information Standards 4-7

JTA SECTION 5 - HUMAN-COMPUTER INTERFACES 5-1

5.1 INTRODUCTION 5-1
5.1.1 Purpose 5-1
5.1.2 Scope 5-1
5.1.3 Background 5-1
5.2 MANDATES 5-2
5.2.1 General 5-2
5.2.2 Style Guides 5-2
5.2.2.1 Commercial Style Guides 5-3
5.2.2.2 DoD Human-Computer Interface (HCI) Style Guide 5-3
5.2.2.3 Domain-level Style Guides 5-4
5.2.2.4 System-level Style Guides 5-4
5.3 EMERGING STANDARDS 5-4

JTA SECTION 6 - INFORMATION SYSTEMS SECURITY STANDARDS 6-1

6.1 INTRODUCTION 6-1
6.1.1 Purpose 6-1
6.1.2 Scope 6-1
6.1.3 Background 6-1
6.2 MANDATES 6-2
6.2.1 Introduction 6-2
6.2.2 Information Processing Security Standards 6-2
6.2.2.1 Application Software Entity Security Standards 6-2
6.2.2.2 Application Platform Entity Security Standards 6-2
6.2.2.2.1 Data Management Services 6-3
6.2.2.2.2 Operating System Services Security 6-3
6.2.2.2.2.1 Security Auditing and Alarms Standards 6-3
6.2.2.2.2.2 Authentication Security Standards 6-3
6.2.3 Information Transfer Security Standards 6-3
6.2.3.1 End System Security Standards 6-3
6.2.3.1.1 Host Security Standards 6-3
6.2.3.1.1.1 Security Algorithms 6-4
6.2.3.1.1.2 Security Protocols 6-4
6.2.3.1.1.3 Evaluation Criteria Security Standards 6-5
6.2.3.2 Network Security Standards 6-5

6.2.3.2.1 Internetworking Security Standards 6-5
6.2.3.3 Transmission Media Security Standards 6-5
6.2.4 Information Modeling And Information Security Standards 6-5
6.2.5 Human-Computer Interface (HCI) Security Standards 6-5
6.3 EMERGING STANDARDS 6-6
6.3.1 Introduction 6-6
6.3.2 Information Processing Security Standards 6-6
6.3.2.1 Application Software Entity Security Standards 6-6
6.3.2.1.1 Evaluation Criteria Security Standards 6-6
6.3.2.1.2 World Wide Web Security Standards 6-6
6.3.2.2 Application Platform Entity Security Standards 6-6
6.3.2.2.1 Software Engineering Services Security 6-7
6.3.2.2.1.1 Generic Security Service (GSS)-Application Program Interface (API) Security 6-7
6.3.2.2.1.2 POSIX Security Standards 6-7
6.3.2.2.2 Operating System Services Security 6-7
6.3.2.2.2.1 Evaluation Criteria Security Standards 6-7
6.3.2.2.2.2 Authentication Security Standards 6-7
6.3.2.2.3 Distributed Computing Services Security Standards 6-8
6.3.3 Information Transfer Security Standards 6-8
6.3.3.1 End System Security Standards 6-8
6.3.3.1.1 Host Security Standards 6-8
6.3.3.1.1.1 Security Protocols 6-8
6.3.3.1.1.2 Public Key Infrastructure Security Standards 6-8
6.3.3.2 Network Security Standards 6-9
6.3.3.2.1 Internetworking Security Standards 6-9
6.3.4 Information Modeling and Information Security Standards 6-9
6.3.5 Human-Computer Interface (HCI) Security Standards 6-9

JTA APPENDIX A - ACRONYMS A-1

JTA APPENDIX B - LIST OF MANDATED STANDARDS AND SOURCES B-1

Information Processing Mandated Standards B-2
Information Transfer Mandated Standards B-6
Information Modeling and Information Mandated Standards B-13
Human-Computer Interfaces Mandated Standards B-14
Information Systems Security Mandated Standards B-15
DOCUMENT SOURCES B-17
Commercial Documents B-17
Government Documents B-17

JTA APPENDIX C - JTA RELATIONSHIP TO DOD STANDARDS REFORM C-1

C.1 DOD (SPECIFICATIONS AND) STANDARDS REFORM - BACKGROUND C-1
C.2 THE JTA AND THE DOD STANDARDS REFORM C-1
C.3 REFORM WAIVER POLICY C-1
C.4 NON-DoDISS DOCUMENTS NOT SUBJECT TO THE REFORM WAIVER POLICY C-2
C.5 INTERFACE STANDARDS ARE WAIVER-FREE C-2
C.6 NON-GOVERNMENT STANDARDS VS MILITARY/FEDERAL STANDARDIZATION DOCUMENTS C-2

USMC SUPPLEMENT USMC-1

USMC 1.1 INTRODUCTION USMC-1

USMC 1.1.1 Purpose USMC-1
USMC 2.1 MANDATES USMC-1
USMC 2.1.1 Introduction USMC-1
USMC 2.1.2 Information Processing Standards USMC-1
USMC 2.1.2.1 Minimum Desktop Computer Configuration and Software Product Requirements USMC-1
USMC 2.1.2.2 Marine Corps Software USMC-4
USMC 2.1.3 Information Transfer Standards USMC-5
USMC 2.1.4 Information Modeling and Information Standards USMC-5
USMC 2.1.5 Human-Computer Interface USMC-5
USMC 2.1.6 Information Systems Security Standards USMC-5
USMC 3.1 EMERGING STANDARDS USMC-5

FREQUENTLY ASKED QUESTIONS (FAQ) ON JTA FAQ-1

JTA SECTION 1 - OVERVIEW

The Warfighter battlespace is complex and dynamic, requiring timely and clear decisions by all levels of military command. There is an unprecedented increase in the amount of data and information necessary to conduct operational planning and combat decision making. Information concerning targets, movement of forces, condition of equipment, levels of supplies, and disposition of assets, both friendly and unfriendly, must be provided to joint commanders and their forces. Therefore, information must flow efficiently between all tactical, strategic, and supporting establishment elements.

As shown in Figure 1-1, Warfighters must be able to work together within and across Services in ways not totally defined in today's operational concepts and/or architectures. They must be able to obtain and use intelligence from theater and National assets which may be processed in forward areas or Continental United States (CONUS). Today's split base/reach back concept requires them to obtain their logistics and administrative support from both home bases and deployed locations. All of this requires that information quickly and seamlessly flow among DoD's sensors, processing and command centers and shooters to achieve dominant battlefield awareness and move inside the enemy's decision loop.

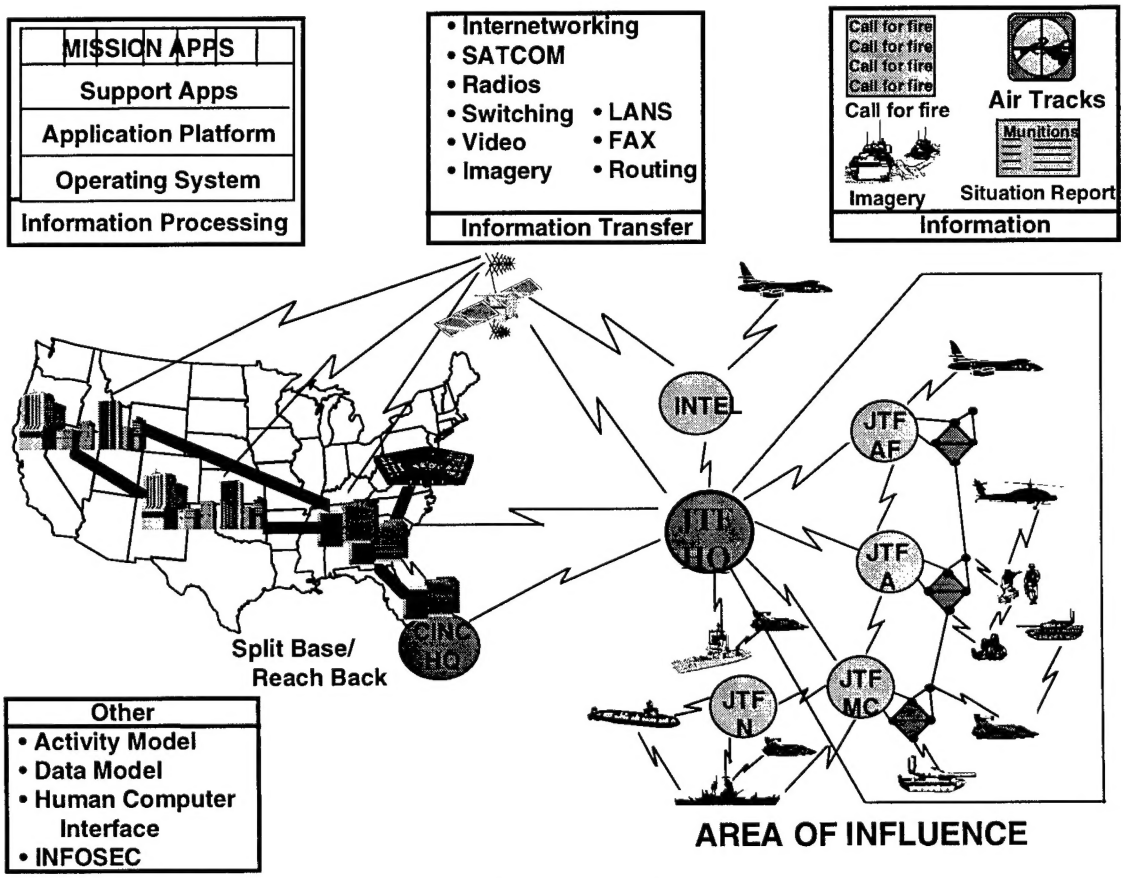


Figure 1-1. Joint Technical Architecture Concept

The Joint Technical Architecture (JTA) provides the "building codes" which, when implemented, permit this flow of information in support of the Warfighter. As shown in Figure 1-1, there must be a distributed information processing environment in which applications are integrated. The applications and data must be independent of hardware to achieve true "plug and play". Information transfer assets must ensure seamless communications within and across diverse media. The information must be in a common format

and have a common meaning. There must also be common human-computer interfaces for users and effective means to protect the information.

1.1 INTRODUCTION

This document, the DoD JTA, mandates the minimum set of standards and guidelines for all DoD Command, Control, Communications, Computers, and Intelligence (C4I) systems acquisition. A foremost objective of the JTA is to improve and facilitate the ability of our systems to support joint and combined operations in an overall investment strategy.

The purpose of this section is to provide an overview of the JTA. It describes the purpose, scope, and background of the JTA in addition to the contents of each section.

1.1.1 Purpose

The purpose of the DoD JTA is:

- To provide the foundation for a seamless flow of information and interoperability among all tactical, strategic, and sustaining base systems that produce, use, or exchange information electronically.

- To mandate standards and guidelines for system development and acquisition which will significantly reduce cost, development time, and fielding time for improved systems, while minimizing the impact on program performance wherever possible.

- To influence the direction of the information industry's standards-based product development by stating the DoD's direction and investment so that information industry's development can be more readily leveraged in systems within DoD.

- To communicate DoD's intent to use open systems products and implementations to industry. DoD will buy commercial products and systems, which use open standards, to obtain the most value for limited procurement dollars.

1.1.2 Background

The evolution of national military strategy in the post cold war era and the lessons learned from the recent conflicts of Desert Shield/ Desert Storm have resulted in a new vision for the DoD. This new vision is commonly known as C4I For The Warrior. Its principle objective is to make information available to the warrior at any time and from any place in order to maximize the effectiveness of the forces and provide a decisive edge in combat. Each of the Services articulated their view of the new doctrine in separate strategy documents: The Enterprise Vision, Army; Horizon, Air Force; Copernicus, Navy; Marine Air Ground Task Force (MAGTF)/C4I, Marine Corps.

Recognizing the need for jointness in combat and the reality of a shrinking budget, the Assistant Secretary of Defense (ASD) Command, Control, Communications, and Intelligence (C3I) issued a memorandum on 14 November 1995 to Service and Agency principals involved in the development of C4I systems. This directive tasked them to "reach a consensus of a working set of standards" and "establish a single, unifying DoD technical architecture that will become binding on all future DoD C4I acquisitions" so that "new systems can be born joint and interoperable, and existing systems will have a baseline to move towards to ensure interoperability."

A Joint Technical Architecture Working Group (JTAWG), chaired by ASD (C3I), C4I Integration Support Activity, was formed and its members agreed to use the Army's Technical Architecture (ATA) as the starting point for the JTA.

1.1.3 Architectures Defined

An architecture is defined in IEEE 610.12 as the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. DoD has implemented this by defining an interrelated set of architectures: Operational, Systems, and Technical. The diagram below shows the relationship among the three architectures. The definitions are provided here to ensure a common understanding of the different types of architectures.

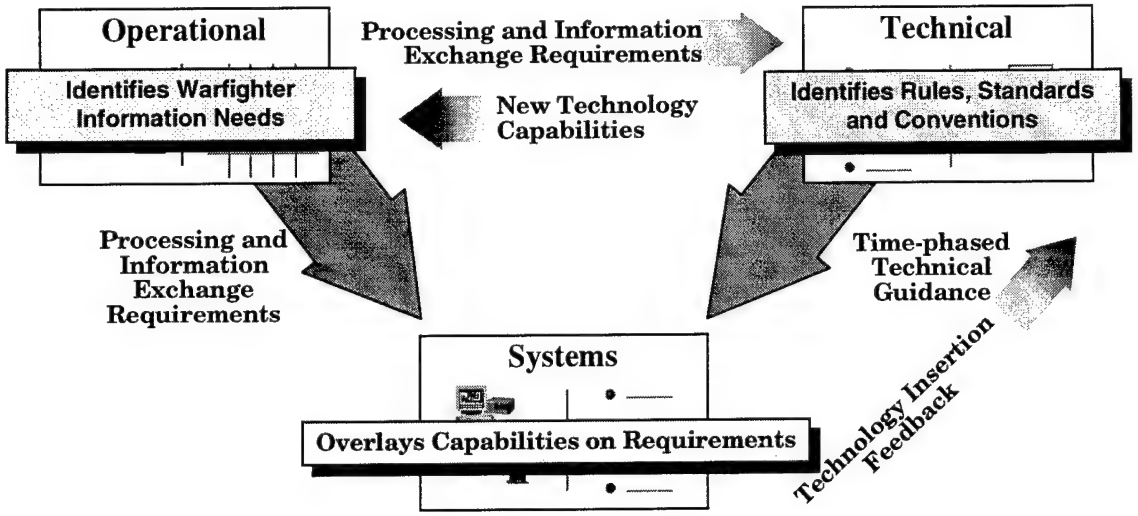


Figure 1-2. Architecture Relationships

1.1.3.1 Operational Architecture (OA)

A description (often graphical) of the operational elements, assigned tasks, and information flows required to accomplish or support the warfighting function. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges.

1.1.3.2 Systems Architecture (SA)

A description, including graphics, of systems* and interconnections** providing for or supporting warfighting functions (C4SR ITF Integrated Architecture Panel, 18 December 1995). The SA defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters. It is constructed to satisfy Operational Architecture requirements per standards defined in the Technical Architecture. The SA shows how multiple systems within a subject area link and interoperate, and may describe the internal construction or operations of particular systems within the architecture. (C4 Chiefs Consensus SA Definition, 12 January 1996, as modified at the suggestion of the USD(A&T) community).

---

* Systems: People, machines, and facilities organized to accomplish a set of specific functions (FIPS PUB 3), which cannot be further subdivided while still performing required functions. Includes the radios, terminals, command, control, and support facilities, sensors and sensor platforms, automated information systems, etc., necessary for effective operations.

** Interconnections: The manual, electrical, or electronic communications paths/linkages between the systems. Includes the circuits, networks, relay platforms, switches, etc., necessary for effective communications.

1.1.3.3 Technical Architecture (TA)

A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

1.1.4 Scope

The scope of JTA Version 1.0 is focused on C4I systems defined for this document as command, control and intelligence systems (to include sustaining base, combat support information systems, and office automation systems) and the communications and computers that directly support them. The JTA also includes the interfaces of those systems with other key assets (e.g., weapon systems, sensors, and models and simulations) to support critical joint Warfighter interoperability.

The JTA is considered a living document and will be updated periodically with continued Service/Agency participation. The JTA's ultimate scope applies to all systems that produce, use, or exchange information electronically. Future versions of the JTA will extend the Version 1.0 scope into other domains and/or focus areas (e.g., weapon systems, sensors, and models and simulations). This extension is critical to truly achieving the objective seamless integration environment envisioned in the C4I For the Warrior concept as documented in Joint Pub 6-0. Achieving and maintaining this vision requires interoperability:

- Within a Joint Task Force/Commander in Chief (CINC)
- Across CINC boundaries
- Between strategic and tactical C4I systems
- Within and across Services and Agencies
- From the battlefield to the sustaining base
- Between US and Coalition forces
- Across current and future systems.

1.1.5 Applicability

The JTA implements DoD Directive (DoDD) 4630.5, which directs that all C4I systems shall be considered for joint use. The JTA shall be used by anyone involved in the management, development, or acquisition of new or improved C4I systems within DoD. Specific guidance for implementing this JTA is provided separately. System developers shall use the JTA to ensure that new and upgraded C4I systems (and the interfaces to such systems) meet interoperability requirements. System integrators shall use it to facilitate the integration of existing and new systems. Operational requirements developers shall be cognizant of the JTA in developing requirements and functional descriptions. When developing C4I applications for Advanced Technology Demonstrations (ATDs), the science and technology community should use the JTA whenever possible to provide the logical interfaces to existing C4I, so that their good ideas will readily integrate into existing systems rather than require massive redesign to meet DoD's interoperability objectives. The JTA is applicable to Advanced Concept Technology Demonstrations (ACTDs).

1.1.6 Key Considerations in Using the JTA

In general, the JTA shall be used to determine the specific standards to be implemented within new or upgraded C4I systems. However, there are several key considerations in using the JTA.

First, the mandatory standards in the JTA must be implemented by systems that have a NEED for the corresponding services. That is, a standard is mandatory in the sense that IF a service/interface is going to be implemented, it shall be implemented in accordance with the associated standard. If a required service can be obtained by implementing more than one standard (e.g., satellite standards), the appropriate standard should be selected based on system requirements.

Second, the JTA is a "forward-looking" document. It guides the acquisition and development of new and emerging C4I functionality and provides a baseline towards which existing systems will move. It is NOT a catalog of all information technology standards used within today's DoD systems. It represents those standards (for interfaces/services) that should be used now and in the future. If legacy standards are needed to interface with existing systems, they can be implemented on a case-by-case basis in addition to the mandated standard.

Third, specification of any other standards (outside of those identified in the JTA) must be additive, complementary, and non-conflictive with JTA mandated standards. Refer to the TAFIM Volume 7 for adopted standards in areas not addressed by the JTA.

1.1.7 JTA Relationship to DoD Standards Reform

The DoD Standards Reform was begun in June 1994 when the Secretary of Defense issued his memorandum entitled "Specifications and Standards - A New Way of Doing Business." This memorandum directs that performance-based specifications and standards or nationally-recognized private sector standards be used in future acquisitions. The intent of this initiative is to eliminate non-value added requirements, and thus to reduce the cost of weapon systems and materiel, remove impediments to getting commercial state-of-the-art technology into our weapon systems, and integrate the commercial and military industrial bases to the greatest extent possible.

The JTA implements standards reform by selecting the minimum standards necessary to achieve joint interoperability. The JTA mandates commercial standards and practices to the maximum extent possible. Use of JTA mandated standards or specifications in acquisition solicitations will not require a waiver from standards reform policies. All mandatory documents in the JTA are of the types that have been identified by the Reform as waiver-free or an exemption has already been obtained. Additional information on this topic can be found in Appendix C.

1.1.8 Basis for the Joint Technical Architecture

While the ATA was the starting point for the JTA, many additions/deletions, reformatting, and other changes led to the current version of the JTA. These changes were the result of strong Service/Agency participation in producing the JTA. In developing the JTA, these participants were able to exploit the work and results of the many other ongoing related technical efforts within the DoD. Among these other efforts are: the Technical Architecture Framework for Information Management (TAFIM), the Defense Information Infrastructure (DII) Common Operating Environment (COE) as documented in the Integration and Runtime Specification (I&RTS), the Air Force Technical Reference Codes (TRCs) , the Navy Computer Resources Management (CRM) , the Marine Corps MAGTF/C4I Technical Architecture, the DoD Index of Specifications and Standards (DoDISS) Profile of the DoD TAFIM, the emerging Intelligence Community Standards, Conventions and Guidelines, and functional profiles such as those developed for the United States Imagery System.

The standards selection criteria used in developing the JTA generally focused on mandating only those items critical to interoperability that were based primarily on commercial open system technology, were implementable, and had strong support in the commercial marketplace. The specific guidance given in selecting standards was that standards would only be mandated if they meet all of the following criteria:

- **INTEROPERABILITY AND/OR BUSINESS CASE:** They ensure joint Service/Agency information exchange and support joint (and potentially combined) C4I operations, and/or there is strong economic justifications that the absence of a mandated standard will result in duplicative and increased life-cycle costs.
- **MATURITY:** They are technically mature and stable.
- **IMPLEMENTABILITY:** They are technically implementable.
- **PUBLIC:** They are publicly available (e.g., open system standards).
- **CONSISTENT WITH AUTHORITATIVE SOURCES:** They are consistent with law, regulation, policy, and guidance documents.

The order of preference used to select the standards follows. Standards that are commercially supported in the marketplace with validated implementations available in multiple vendors' mainstream commercial products took precedence. Publicly held standards were generally preferred. International or national industry standards were preferred over military or other government standards.

Many standards have optional parts or parameters that can affect interoperability. In some cases, a standard may be further defined by a standards profile which requires certain options to be present to ensure proper operation and interoperability.

The word "Standards" as referred to in the JTA is a generic term for the collection of documents cited herein. "Standards" as cited in the JTA may include commercial, federal and military standards and specifications, and various other kinds of documents and publications.

1.1.9 JTA Relationships

As discussed, there are several key efforts (i.e., TAFIM, Service/Agency technical architectures and the COE) related to the JTA. The TAFIM provides the processes and framework for defining Version 1.0 of the JTA. For the C4I domain, the JTA set of standards supersedes those listed in the TAFIM. As the JTA evolves, its relationship to these key efforts is likely to change.

Previously, each of the Services, Agencies and the Intelligence Community, has established their own sets of standards (e.g., technical architectures). The JTA is envisioned as "...a single, unifying DoD technical architecture..." in the ASD(C3I) 1995 memo, which Services and Agencies will supplement as necessary.

Finally, the DII COE is the specific COE implementation that will continue to evolve in compliance with all applicable JTA specifications, standards, and source references.

1.2 DOCUMENT ORGANIZATION

The JTA's body consists of six main sections. The first section is the overview. The next five are: (2) Information Processing Standards; (3) Information Transfer Standards; (4) Information Modeling and Information Standards; (5) Human-Computer Interfaces; and (6) Information Systems Security Standards.

The JTA identified in the main body of this document is mandated for all DoD Services and Agencies, but supplements apply only to the specific Service/Agency identified. The supplement(s) address Technical Architecture additions for specific organizational entities within DoD. The JTA always takes precedence over supplements.

1.2.1 General

Each section, except for the overview, is divided into three subsections as follows:

- Introduction - This subsection is for informational purposes only. It defines the purpose and scope of the subsection and provides background descriptions and definitions that are unique to the section.

- Mandates - This subsection identifies mandatory standards, profiles, and practices. Each mandated standard or practice is clearly identified on a separate line and includes a formal reference citation that can be included within Requests for Proposals (RFP) or Statements of Work (SOW).

- Emerging - This subsection provides an abbreviated description of candidates to be added to or to replace adopted standards. This includes standards required to capitalize on new technologies. The purpose of listing these candidates is to help the program manager determine those areas that are likely to change in the near term (within three years) and suggest those areas in which "upgradability" should be a concern. The expectation is that emerging standards will be elevated to mandatory status when implementations of the standards mature. Emerging standards may be implemented, but shall not be used in lieu of a mandated standard.

1.2.2 Information Processing Standards

Section 2 mandates government and commercial information processing standards the DoD shall use to develop integrated, interoperable systems that meet the Warfighter's information processing requirements. This section also describes the DII COE concept and individual processing standards.

1.2.3 Information Transfer Standards

Section 3 describes the information transfer standards and profiles that are essential for information transfer interoperability and seamless communications. This section mandates the use of the open-systems standards used for the Internet and the Defense Information Systems Network (DISN). These networks use the Internet Protocol (IP) suite, which provides communications interoperability between information systems that are on different platforms or communications networks.

1.2.4 Information Modeling and Information Standards

Section 4 describes the use of integrated information modeling and mandates applicable standards. Information modeling consists of Activity and Data Modeling. This section explains the use of the DoD Command and Control (C2) Core Data Model (C2CDM) and the Defense Data Dictionary System (DDDS), formerly the Defense Data Repository System (DDRS). This section also mandates information standards including message formats.

1.2.5 Human-Computer Interfaces

Section 5 provides a common framework for Human-Computer Interface (HCI) design and implementation in DoD automated systems. The objective is the standardization of user interface implementation options, enabling DoD applications to appear and behave in a reasonably consistent manner. The section specifies HCI design guidance, mandates, and standards.

1.2.6 Information Systems Security Standards

Section 6 prescribes the standards and protocols to be used to satisfy security requirements. This section provides the mandated and emerging security standards that apply to JTA Sections 2 through 5. Section 6 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related JTA subject areas.

1.2.7 Appendices

The appendices provide supporting information (e.g., how to get a copy of mandated standards) and available links to standards organization's home pages, which facilitate the use of the document, but are not mainline to the purpose of the document.

1.2.8 Annexes

Annexes provide extensions to the Technical Architecture necessary for a specific domain. Additional annexes will be added as other non-C4I domain Technical Architectures are addressed. Annexes are organized in the same way as the subsections of the JTA. Each includes an introduction clearly specifying the purpose, scope, and background of the annex. Annexes identify mandated standards within a framework that follows the JTA structure. They may also address emerging standards that are of interest to the domain or organization. There are currently no annexes to the JTA.

1.2.9 Supplements

Supplements address Technical Architecture additions for specific organizational entities within DoD. Each supplement includes an introduction clearly specifying the purpose, scope, and background of the supplement. Supplements identify mandated standards within a framework that follows the JTA structure. They may also address emerging standards that are of interest to the organization.

The JTA is mandated for all DoD Services and Agencies while supplements are mandated only for the specific Service/Agency that prepares the supplement. The JTA always takes precedence over supplements. Supplements are submitted by a Service or Agency, but are subject to joint review to ensure the supplements are within the scope of the JTA and are consistent with the approved mandates.

1.3 CONFIGURATION MANAGEMENT

The JTA will be jointly configuration managed by the CINCs, Services and Agencies.

Proposed changes should be provided to the JTA point of contact identified by your CINC/Service/Agency. Changes may also be submitted via jta-comment@itsi.disa.mil. Changes received via jta-comment@itsi.disa.mil will be referred to your CINC/Service/Agency JTA point of contact. Industry and non-DoD comments should be submitted through the Defense Information Systems Agency (DISA) Center for Standards (CFS) via jta-comment@itsi.disa.mil.

JTA SECTION 2 - INFORMATION PROCESSING STANDARDS

2.1 INTRODUCTION

2.1.1 Purpose

The purpose of this section is to specify the Joint Technical Architecture (JTA) government and commercial information processing standards the DoD will use to develop integrated, interoperable systems that directly or indirectly support the Warfighter.

Information processing standards support the objectives of reducing cost and time of development, easing software integration and maintenance, and improving interoperability. The primary mechanism is the concept of a Common Operating Environment (COE) that provides a reusable set of common software services via standard application program interfaces (APIs). By building modular applications that use a common software infrastructure accessed through a stable set of APIs, as well as a standard integration approach, developers will be able to "plug and play" their applications into a centrally maintained infrastructure. The use of the standard APIs allows the COE and mission applications to be quickly integrated, and updated relatively independent of each other. The COE concept allows developers to concentrate their efforts on building mission area applications rather than building duplicative system service infrastructure software. Common standards, such as SQL to communicate with relational database management systems and Computer Graphics Metafile (CGM) to store graphics, support the objective of interoperability. Systems developed to these standards will be able to share services (retrieve authorized data from each other's databases) and data (such as an overlay). The use and evolution of the COE concept and the JTA standards it embodies, will advance the goal of building systems that are compatible, while minimizing program costs through systematic software reuse.

2.1.2 Scope

This section applies to mission area, support application, and application platform service software. This section does not cover communications standards needed to transfer information between systems (refer to Section 3), nor standards relating to information modeling (process, data, and simulation), data elements, or military unique message set formats (refer to Section 4).

2.1.3 Background

The COE Concept is described in the Integration and Runtime Specification (I&RTS), Version 2.0, October 1995. The Defense Information Infrastructure (DII) COE is implemented with a set of modular software that provides generic functions or services, such as operating system services. These services or functions are accessed by other software through standard APIs. The DII COE may be adapted and tailored to meet the specific requirements of a domain. The key is that domain implementations adhere to the COE concept in that they provide standard modularized software services that are consistent with the Technical Architecture Framework for Information Management (TAFIM) Technical Reference Model (TRM) and that application programmers have access to these services through standard APIs.

The individual standards contained in this section and applicable appendices that will be used to implement a domain COE are presented within the framework of the TAFIM TRM. This reference model was intentionally generalized and does not imply any specific system architecture. Its purpose is to provide a "set of concepts, entities, interfaces, and diagrams that provides a basis for the specification of standards." The TAFIM TRM organizes software into two entities, an Application Software Entity and an

Application Platform Entity. The Application Software Entity communicates with the Application Platform Entity through an API. The Application Platform Entity communicates with the external environment through the External Environment Interface (EEI). The TAFIM TRM decomposes these entities into sub-categories as shown in Figure 2-1. The application software entity and associated mandates are detailed in Section 2.2.1, while the Application Platform's seven major service areas and associated mandates are detailed in Section 2.2.2.1. Section 2.2.2.2 defines the Application Platform Cross-Area Services and their associated mandates.

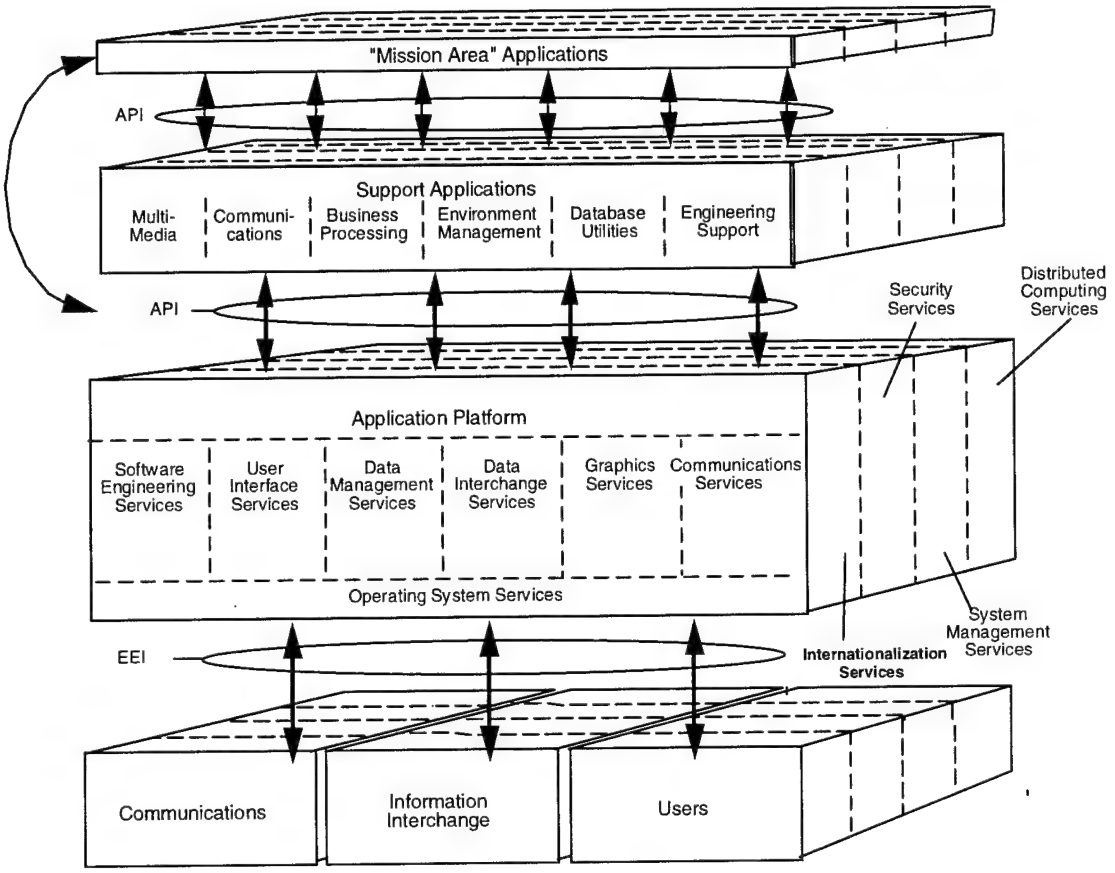


Figure 2-1. Detailed DoD TRM, Version 3.0

2.2 MANDATES

The DII COE, as defined in the DII COE I&RTS Version 2.0, is fundamental to a Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) System Architecture (JCSA). In the absence of a JCSA, the JTA mandates that all Command, Control, Communications, Computers, and Intelligence (C4I) systems shall use the DII COE. All applications of a system which must be integrated into the DII shall be at least DII COE I&RTS level 5 compliant (software is segmented, uses DII COE Kernel, and is installed via COE tools) with a goal of achieving level 8.

The following sections provide the applicable mandates that shall be used in the selection of commercial or government off-the-shelf (GOTS) software or in the development of government software, to include the DII COE. Appendix B contains a table that summarizes the mandated standards from this section, as

well as providing information on how to obtain the standards. The World Wide Web (WWW) version of Appendix B contains a link to the standard or to the organization that maintains the standard when one is available.

2.2.1 Application Software Entity

The Application Software Entity includes both mission area applications and support applications. Mission area applications implement specific user's requirements and needs (e.g., personnel, material, management). This application software may be commercial off-the-shelf (COTS), GOTS, custom-developed software, or a combination of these.

Common support applications are those (e.g., e-mail and word processing) that can be standardized across individual or multiple mission areas and are the first layer of the DII COE. The services they provide can be used to develop mission-area-specific applications or can be made available to the user. The TAFIM TRM defines six support application categories: Multimedia, Communications, Business Processing, Environment Management, Database Utilities, and Engineering Support. The definitions of these categories are found in the TAFIM, Volume 2, Section 2.4.2.

The Application Software Entity includes all DoD application software. The following mandate applies:

- All system developers shall identify their common support applications and mission area applications. Mission area applications shall transition to the DII COE common support applications to the maximum extent possible.

2.2.2 Application Platform Entity

The Application Platform Entity is the second layer of the DII COE, and includes the common, standard services upon which the required functionality is built. The Application Platform Entity is used by the DII COE support applications and unique mission area applications software. The Application Platform Entity is composed of service areas and cross-area services. The definitions of these service areas are found in the TAFIM, Volume 2, Section 2.4.3 and 2.4.4 respectively. The corresponding mandates are provided in the following subsections.

2.2.2.1 Service Areas

The TAFIM TRM defines seven service areas within the Application Platform Entity: Software Engineering, User Interfaces, Data Management, Data Interchange, Graphics, Communications, and Operating System Services.

2.2.2.1.1 Software Engineering Services

The software engineering services provide system developers with the tools that are appropriate to the development and maintenance of applications.

Language services provide the basic syntax and semantic definition for use by developers to describe the desired software function.

According to DoD 5000.2-R, it is DoD policy to design and develop software systems based on software engineering principles. Additional guidance is contained in DoD Directive (DoDD) 3405.1. This mandate does not include software that is developed and maintained commercially.

2.2.2.1.2 User Interface Services

These services implement the Human-Computer Interface (HCI) style and control how users interact with the system. The JTA mandates either Common Desktop Environment (CDE) Version 1.0 based on X Window System and Open Software Foundation (OSF) Motif APIs, or the applicable native windowing Win32 APIs. The following standards are mandated:

- FIPS Pub 158-1: 1993, User Interface Component of the Application Portability Profile X-Windows Version 11, Release 5
- OSF Motif Application Environment Specification (AES), Release 1.2, 1992
- OSF/Motif Inter Client Communications Convention Manual (ICCCM) for communication between Graphical User Interface (GUI) client applications
- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993, Microsoft Press
- X/Open C323, Common Desktop Environment (CDE) Version 1.0, April 1995.

Refer to Section 5 for HCI style guidance and standards.

2.2.2.1.3 Data Management Services

Central to most systems is the sharing of data between applications. The data management services provide for the independent management of data shared by multiple applications.

These services support the definition, storage, and retrieval of data elements from Database Management Systems (DBMSs). Application code using Relational Database Management System (RDBMS) resources and COTS RDBMSs shall conform to the requirements of Entry Level SQL. The following standards are mandated for any system required to use an RDBMS.

- FIPS Pub 127-2: 1993, Database Language for relational DBMSs.

The following API is mandated for both database application clients and database servers:

- Open Data Base Connectivity, ODBC 2.0.

2.2.2.1.4 Data Interchange Services

The data interchange services provide specialized support for the exchange of data and information between applications and to and from the external environment. These services include document, graphics data, geospatial data, imagery data, product data, audio data, video data, atmospheric data, oceanographic data, and compression interchange services.

Message interchange standards are covered in Section 4.

2.2.2.1.4.1 Document Interchange

These services provide the specifications for encoding data and the logical and visual structure of electronic documents. The following standards are mandated for document interchange:

- ISO 8879: 1986, Standard Generalized Markup Language (SGML), for the production of documents which are intended for long-term storage and electronic dissemination for viewing in multiple formats. SGML formalizes document markup, making the document system and processing independently. It is an architecture-free and application-free language for managing structures and is designed for full multi-media database publishing. SGML is a meta-language, providing the rules for designing and applying a system of markup tags rather than the specific set of tags.

- RFC-1866: 1995, Hypertext Mark-up Language (HTML), Internet Version 2.0, - Interchange format used by the WWW for hypertext format and embedded navigational links.

Table 2-1 identifies file formats for the interchange of common document types such as text documents, spreadsheets, and presentation graphics. Some of these formats are controlled by individual vendors, but all of these formats are supported by products from multiple companies. In support of the standards mandated in this section, Table 2-1 identifies conventions for file name extensions for documents of various types. The following file formats are mandated, but not the specific products mentioned:

- All applications acquired or developed for the production of documents shall be capable of generating at least one of the formats listed in Table 2-1 for the appropriate document type.
- All organizations shall at a minimum be capable of reading and printing all of the formats listed below for the appropriate document type.

Table 2-1 - Document Interchange Formats

Document Type	Standard/Vendor Format	Recommended File Name Extension	Reference
Plain Text	ASCII Text	.txt	
Compound Document*	Acrobat 2.0	.pdf	Vendor
	HTML 2.0	.htm	IETF
	MS Word 6.0	.doc	Vendor
	Rich Text Format	.rtf	Vendor
	WordPerfect 5.2	.wp5	Vendor
Briefing - Graphic Presentation	Freelance Graphics 2.1	.pre	Vendor
	MS Powerpoint 4.0	.ppt	Vendor
Spreadsheet	Lotus 1-2-3 Release 3.x	.wk3	Vendor
	MS Excel 5.0	.xls	Vendor
Database	Dbase 4.0	.dbf	Vendor

Note: * - Compound documents contain embedded graphics, tables, and formatted text. OLE linking complicates document interchange. Note that not all special fonts, formatting, or features supported in the native file format may convert accurately.

Note: Future versions of the JTA will address engineering and technical data standards such as Continuous Acquisition and Life-Cycle Support (CALS).

2.2.2.1.4.2 Graphics Data Interchange

These services are supported by device-independent descriptions of the picture elements for vector and raster graphics. The ISO Joint Photographic Expert Group (JPEG) standard describes several alternative algorithms for the representation and compression of raster images, particularly for photographs. The standard does not specify an interchange format for JPEG images, which led to the development of the JPEG File Interchange Format (JFIF) format. JFIF is a de facto standard for exchanging images over the internet. The following standards are mandated:

- FIPS Pub 128-1: 1993, Computer Graphics Metafile (CGM)- Interchange format for vector graphics data
- JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems for raster graphics data encoded using the ISO 10918-1: 1994, Joint Photographic Expert Group (JPEG) algorithm.

2.2.2.1.4.3 Geospatial Data Interchange

For mapping, charting, and geodesy (MC&G) services, collectively known as geospatial services, the following standards are mandated:

- MIL-STD-2411, Raster Product Format (RPF) - DoD Military Standard used by the Defense Mapping Agency (DMA) to format raster-based digital products (e.g., Compressed Arc Digitized Raster Graphics (CADRG), Controlled Image Base (CIB), and Digital Point Positioning Data Base (DPPDB)), and is based on National Imagery Transmission Format Standard (NITFS) (MIL-STD-2500A) described below.
- MIL-STD-2407, Interface Standard for Vector Product Format (VPF) - DoD format for DMA's vector-based products used by geographic information system (GIS) and other DoD systems. VPF standard products include Vector Map (VMap) Levels 0-2, Urban Vector Map (UVMap), Digital Nautical Chart (DNC), VMap Aeronautical Data (VMap AD), Vector Product Interim Terrain Data (VITD), Digital Topographic Data (DTOP), Littoral Warfare Data (LWD), and World Vector Shoreline Plus (WVS+).
- MIL-STD-2401, World Geodetic System 84 (WGS-84) 21 March 1994 - DoD's standard global reference system developed by the DMA. WGS-84 is employed by the NAVSTAR Global Positioning System (GPS) and modern weapons and systems. Latitude and longitude data shall use WGS-84 in accordance with CJCSI 3900.01, and standard coordinate data elements as discussed in Section 4.
- For all other MC&G services (e.g., Digital Terrain Elevation Data (DTED), Digital Bathymetric Database (DBDB)) not captured in the above standards the products in DMAL 805-1A, DMA List of Products and Services, March 1994, shall be used.

2.2.2.1.4.4 Imagery Data Interchange

The NITFS is a DoD and Federal Intelligence Community suite of standards for the exchange, storage, and transmission of digital imagery products. NITFS provides a package containing information about the image, the image itself, and optional overlay graphics. It was developed and mandated by ASD Command, Control, Communications, and Intelligence (C3I) for the dissemination of digital imagery from overhead collection platforms. Guidance on applying the suite of standards can be found in MIL-HDBK-1300A. The following standards are mandated for secondary imagery dissemination:

- MIL-STD-2500A, National Imagery Transmission Format (Version 2.0) for file format
- MIL-STD-188-196, Bi-Level Image Compression
- MIL-STD-188-199, Vector Quantization Decompression
- ANSI/ISO 8632: 1992, Computer Graphics Metafile (CGM) as profiled by FIPS 128 and MIL-STD-2301
- ISO/IEC 10918-1: 1994, Joint Photographic Experts Group (JPEG) as profiled by MIL-STD-188-198A. Although the NITFS uses the same ISO JPEG algorithm as mandated in section 2.2.2.1.4.2, the NITFS file format is not interchangeable with the JFIF file format.

Communication protocols for transmission of imagery are specified in Section 3.

2.2.2.1.4.5 Product Data Interchange

Product Data Interchange standards will be addressed in a later version of the JTA.

2.2.2.1.4.6 Audio Data Interchange

Formats for the exchange of stand-alone audio will be addressed in a later version of the JTA.

MPEG-1 audio is not a single compression algorithm but a family of three audio encoding and compression schemes called MPEG-Audio Layer-2, and Layer-3, all three of which are hierarchically compatible. The audio compression schemes are lossy, but they can achieve perceptually lossless quality. The following standards are mandated for audio in conjunction with MPEG-1 video:

- ISO/IEC 11172-1: 1993 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems
- ISO/IEC 11172-3: 1993 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 3: Audio
- ISO/IEC 11172-3/Cor. 1: 1995 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 3: Audio Technical Corrigendum.

MPEG-2 audio is intended to encode up to five full bandwidth channels (left, right, center, and two surround channels), and additional low-frequency enhancement channel, and up to seven commentary or multilingual channels. The following standards are mandated for audio in conjunction with MPEG-2 video:

- ISO 13818-1: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems
- ISO 13818-3: 1995 - Generic Coding of Moving Pictures and Associated Audio Information - Part 3: Audio.

2.2.2.1.4.7 Video Data Interchange

MPEG-1 provides for a wide range of video resolutions and data rates but is optimized for single and double-speed CD-ROM data rates (1.2 and 2.4 Mbits/s). With 30 frames per second video at a display resolution of 352 x 240 pixels, the quality of compressed and decompressed video at this data rate is often described as similar to VHS recording. MPEG-1 is frequently used in applications with limited bandwidth, such as CD-ROM playback or Integrated Services Digital Network (ISDN) videoconferencing. The following standards are mandated:

- ISO/IEC 11172-1: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems
- ISO/IEC 11172-1: 1993/Cor. 1:1995 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems Technical Corrigendum 1
- ISO/IEC 11172-2: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 2 Video.

MPEG-2 is designed for the encoding, compression, and storage of studio-quality motion video and multiple CD-quality audio channels at bit rates of 4 to 6 Mbits/s. MPEG-2 has also been extended to cover HDTV. The following standards are mandated:

- ISO 13818-1: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems
- ISO 13818-2: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video.

Video Teleconferencing (VTC) standards are specified in Section 3.

2.2.2.1.4.8 Atmospheric Data Interchange

The following formats established by the World Meteorological Organization (WMO) Commission for Basic Systems (CBS) for meteorological data and published under the Manual for Codes, Volume 1, Part B, Binary Codes, WMO No. 306. The following standards are mandated:

- FM 92-X-GRIB - The WMO Format for the Storage of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form. GRIB was developed for the transfer of gridded data fields, including spectral model coefficients, and of satellite images. A GRIB record (message) contains values at grid points of an array, or a set of spectral coefficients, for a parameter at a single level or layer as a continuous bit stream. It is an efficient vehicle for transmitting large volumes of gridded data to automated centers over high speed telecommunication lines using modern protocols. It can equally well serve as a data storage format. While GRIB can use predefined grids, provisions have been made for a grid to be defined within the message.
- FM 94-X-BUFR - The WMO Binary Universal Format for Representation (BUFR) of meteorological data. Besides being used for the transfer of data, BUFR is used as an on-line storage format and as a data archiving format. A BUFR record (message) containing observational data of any sort also contains a complete description of what those data are: the description includes identifying the parameter in question, (height, temperature, pressure, latitude, date, and time), the units, any decimal scaling that may have been employed to change the precision from that of the original units, data compression that may have been applied for efficiency, and the number of binary bits used to contain the numeric value of the observation. BUFR is a purely binary or bit oriented form.
- Data Exchange Format (DEF) - Appendix 30 to the Tactical Automated Weather Distribution System (TAWDS)/Integrated Meteorological System (IMETS) Implementation Document for Communication Information Data Exchange (CIDE).

2.2.2.1.4.9 Oceanographic Data Interchange

Standard transfer formats are required for the pre-distribution of oceanographic information. WMO GRIB and the BUFR file transfer formats are used for this purpose. The GRIB and BUFR extensions include several extensions, including provision for additional variables, additional originating models, a standard method to encode tables and line data; a method to encode grids (tables) with an array of data at each grid point (table entry); and a method to encode multiple levels in one GRIB message. There is also a possible need to incorporate a method for vector product data. The following WMO CBS format for oceanographic data use is mandated:

- FM 94-X-BUFR - The WMO Binary Universal Format for Representation (BUFR) of oceanographic data.

2.2.2.1.4.10 Compression

General compression standards will be included in a later version of the JTA. See Section 2.2.2.1.4.4 for imagery compression standards.

2.2.2.1.5 Graphic Services

These services support the creation and manipulation of graphics. They include device-independent, multidimensional graphic object definition, and the management of hierarchical database structures containing graphics data. The following standards are mandated for non-COTS graphics development:

- ISO 7942 as profiled by FIPS Pub 120-1 (change notice 1): 1991, Graphical Kernel System (GKS) - for 2-D graphics
- ISO 9592: 1989, as profiled by FIPS Pub 153, Programmers Hierarchical Interactive Graphics Systems (PHIGS) - for 3-D graphics

- ISO/IEC 9636: 1994, Information Technology-Computer Graphics-Interfacing (CGI) Techniques for Dialogue with Graphics Devices.

2.2.2.1.6 Communications Services

These services support the distributed applications that require data access and applications interoperability in networked environments. The mandated standards are provided in Section 3.

2.2.2.1.7 Operating System Services

These core services are necessary to operate and administer a computer platform and to support the operation of application software. They include kernel operations, shell, and utilities. The kernel controls access to information and the underlying hardware. These services shall be accessed by applications through either the standard Portable Operating System Interface (POSIX) or WIN32 APIs. Not all operating system services are required to be implemented, but those that are used shall comply with the standards listed below.

The following standards are mandated:

- ISO 9945-1: 1990, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API) [C language]*, (as profiled by FIPS PUB 151-2: 1994)
- ISO 9945-2: 1993, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities, (as profiled by FIPS PUB 189: 1994)
- IEEE 1003.2d: 1994, POSIX - Part 2: Shell and Utilities - Amendment: Batch Environment
- IEEE 1003.1b: 1993, POSIX - Part 1: System Application Program Interface (API) Amendment 1; Real Time Extension [C Language]*, (as profiled by FIPS Pub 151-2: 1993)
- IEEE 1003.1i: 1995, POSIX - Part 1: System Application Program Interface (API) Amendment: Technical Corrigenda to Real-time Extension [C Language]*
- IEEE 1003.1c: 1995, POSIX - Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]*
- Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993, Microsoft Press.

Note: * - The reference to C Language is part of the formal title of these standards. It denotes the language used to define the standard.

2.2.2.2 Application Platform Cross-Area Services

The TAFIM TRM defines four application platform cross-area services: Internationalization, Security, System Management, and Distributed Computing Services. See Figure 2-1.

2.2.2.2.1 Internationalization Services

The internationalization services provides a set of services and interfaces that allow a user to define, select, and change between different culturally related application environments supported by the particular implementation. These services include character sets, data representation, cultural convention, and native language support.

In order to interchange text information between systems, it is fundamental that systems agree on the character representation of textual data. The following character set coding standards, which build upon

the ASCII character set, are mandated for the interchange of 8-bit and 16-bit textual information respectively:

- ISO/IEC 8859-1: 1987, Information Processing - 8-Bit Single-Byte Coded Character Sets - Part 1: Latin Alphabet No. 1
- ISO/IEC 10646-1: 1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane.

2.2.2.2.2 Security Services

These services assist in protecting information and computer platform resources. They must often be combined with security procedures, which are beyond the scope of the information technology service areas, to fully meet security requirements. Security services include security policy, accountability, and assurance. [Note: Security Service standards have been consolidated in Section 6.)

2.2.2.2.3 System Management Services

These services provide capabilities to manage an operating platform and its resources and users. System management services include configuration management, fault management, and performance management. Network Management mandated standards are provided in Section 3.2.1.1.1.5. There are no standards currently mandated for systems management.

2.2.2.2.4 Distributed Computing Services

These services allow various tasks, operations, and information transfers to occur on multiple, physically- or logically-dispersed, computer platforms. These services include, but are not limited to, global time; data, file, and name services; thread services; and remote process services. There are two categories of Distributed Computing Services, Remote Procedure Computing and Distributed Object Computing.

2.2.2.2.4.1 Remote Procedure Computing

The mandated standards for remote procedure computing are identified in the OSF Distributed Computing Environment (DCE) Version 1.1. The mandated standards are:

- OSF - DCE Remote Procedure Call (RPC), Version 1.1, 1994
- OSF - DCE Time Services, Version 1.1, 1994
- OSF - DCE Directory Services, Version 1.1, 1994.

2.2.2.2.4.2 Distributed Object Computing

The mandated standards for distributed object computing are identified within the Object Management Group (OMG) Object Management Architecture (OMA) as described in:

- OMG - The Common Object Request Broker: Architecture and Specification, Version 2: July 1995 (also available as: X/Open Common Application Environment (CAE) Specification P431 - Common Object Request Broker Architecture & Specification, Version 2)
- OMG - CORBA services: Common Object Services Specification, March 1996 (also available as: X/Open CAE Specification P432 - Common Object Services, Volume 1 and X/Open CAE Specification P502 - Common Object Services, Volume 2)
- OMG - CORBA facilities: Common Object Facilities Architecture, November 1995.

2.3 EMERGING STANDARDS

The standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

2.3.1 Software Engineering Service

There are no emerging standards for software engineering services.

2.3.2 User Interface

Within User Interface Services space, the Common Open Software Environment (COSE) attempted to unify the existing GUI standards under a common framework. The result was the COSE CDE Version 1.0. This framework provides not only mechanisms for graphical display of common objects, but it also provides standard interprocess communication mechanisms and a set of commonly-used desktop tools (e.g., file manager and mail tool) that are relevant to many domains. There are a number of vendors who have received X/Open Brands for CDE 1.0. The next version of the CDE technology is being sponsored under the OSF Prestructured Technology (PST) business model. The effort has been designated CDENext.

2.3.3 Data Management

Within Data Management Services, standards for both RDBMS and Object-Oriented Database Management Systems (OODBMSs) will continue to evolve and mature. In the RDBMS domain, SQL3 is being developed by the ANSI X3H2 committee. In the OODBMS domain, the Object Database Management Group (ODMG) is evolving from the ODMG-93 specification to the ODMG-9x standard. SQL3 and ODMG-9x are being developed in parallel to ensure as much commonality as possible. Thus, an RDBMS that conforms to SQL3 will be able to access an OODBMS that conforms to ODMG-9x and vice versa. Both specifications are expected to be completed by mid-1997.

ISO 9075-3, 1995 Call Level Interface and DIS 9075-4, Database Language, Part 4: Persistent Stored Modules (SQL/PSM) are emerging standards for application programmer interface with DBMS servers. Open Data Base Connectivity (ODBC) 3.0 (once finalized) is expected to become the de-facto commercial standard for which vendors will build their products in the near future. However, since ODBC 3.0 is expected to support all of the ISO CLI standard, plus additional vendor extensions (not standard), it is an emerging standard for RDBMS procurement.

2.3.4 Data Interchange

Within Data Interchange Services, wavelet techniques are being reviewed for inclusion in the NITFS imaging standard. The ISO 13818-4, MPEG-2 is an interchange format used for full motion video and associated audio data for data rates of 1.5 Mbits/s - 6.0 Mbits/s.

HTML 3.2 is currently in work within the WWW Consortium as the successor to HTML 2.0. HTML 3.2 includes many of the highly desired features such as tables, found in non-standard forms in many vendors' products.

Geospatial standards are migrating from Military Standards to Interface Standards or to Standard Practices, both of which do not require waivers for use. MIL-STD-2405, Datums, Coordinates and Grids is being revised as an Interface Standard in FY96; MIL-STD-600001, Accurace, is slated for conversion to Standard Practices. If either standard is use prior to coversion they will require a waiver.

2.3.5 Operating Systems

Within Operating System Services, it is expected that the draft IEEE P1003.x POSIX standards will be adopted once they become final. The following POSIX drafts will be approved as standards soon:

P1003.1d	Real-Time Extensions
P1003.1h	Services for Reliable, Available, Serviceable Systems
P1003.1g	Protocol Independent Interfaces
P1003.5b	Ada Bindings for Real-Time
P1003.2l	Real-Time Distributed Systems Communication
P1003.1j	Advanced Real-Time Extensions.

The X/Open Single UNIX Specification (SUS) (previously referred to as Specification 1170) is being updated to include POSIX real-time interfaces. Operating systems that conform to this specification and have received the UNIX brand from X/Open are on the market. For UNIX-based implementations, strong emphasis should be placed on acquiring systems that are SUS conformant over those that are not.

JTA SECTION 3 - INFORMATION TRANSFER STANDARDS

3.1 INTRODUCTION

3.1.1 Purpose

Information transfer standards and profiles are described in this section. These standards promote seamless communications and information transfer interoperability for DoD systems.

3.1.2 Scope

This section identifies the interface standards that are required for interoperability between and among Command, Control, Communications, Computers, and Intelligence (C4I) systems, supporting access for data, facsimile, video, imagery, and multimedia systems. Also identified are the standards for internetworking between different subnetworks. Transmission media standards for Synchronous Optical Network (SONET) and radio links are identified. Finally, emerging technologies that should be monitored, for future extension of information transfer capabilities, are identified. This section includes the Communications Services depicted in the TRM, Figure 2-1. Security standards are addressed in Section 6.2.3.

3.1.3 Background

The standards herein are drawn from widely accepted commercial standards when they meet DoD requirements. Where necessary for interoperability, profiles of commercial standards are used. Military standards are mandated only when suitable commercial standards are not available. For example, the Joint Technical Architecture (JTA) makes use of the open-systems architecture used by the Internet and the Defense Information Systems Network (DISN). These networks provide for communications interoperability between end systems that are on different communications subnetworks. System components are categorized here as hosts, subnetworks, and routers. Hosts are computers that generally execute application programs on behalf of users and share information with other hosts via networks. Networks may be relatively simple (e.g., point-to-point links) or have complex internal structures (e.g., network of packet switches). Routers interconnect two or more subnetworks and forward packets across subnetwork boundaries. Routers are distinct from hosts in that they are normally not the destination of data traffic.

3.2 MANDATES

This subsection identifies the mandatory standards, profiles, and practices for information transfer. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards. The World Wide Web (WWW) version of Appendix B contains a link to the standard or to the organization that maintains the standard when one is available.

3.2.1 End System Standards

This subsection addresses standards for the following types of end systems: host, Video Teleconferencing (VTC), facsimile, and secondary imagery dissemination.

3.2.1.1 Host Standards

Internet Architecture Board (IAB) Standard-3 is an umbrella standard that references other documents and corrects errors in some of the referenced documents. Standard-3 also adds additional discussion and guidance for implementors. The following standard is mandated:

- IAB Standard 3/RFC-1122/RFC-1123, Host Requirements, October 1989.

3.2.1.1.1 Application Support Services

3.2.1.1.1.1 Electronic Mail

The standard for electronic mail is the Defense Message System (DMS)'s X.400-based suite of military messaging standards as defined in Allied Communication Publication (ACP) 123 U.S. Supplement No. 1. The U.S. Supplement annexes contain standards profiles for the definition of the DMS "Business Class Messaging" (P772) capability and the Message Security Protocol (MSP). See Section 6 for security standards. Since X.400 is not an internet standard, see 3.2.1.1.2.2 for operation over Internet Protocol (IP) based networks. The following standard is mandated:

- ACP 123 U.S. Supplement No. 1, Common Messaging Strategy and Procedures, November 1995.

3.2.1.1.1.2 Directory Services

X.500 and Domain Name System (DNS) provide complimentary directory services. The X.500 protocol provides individual and organizational directory services and is mandated for use with DMS. The DNS provides computer addressing services and is mandated for Internet Protocol (IP)-based services.

3.2.1.1.1.2.1 X.500 Directory Services

International Telecommunications Union (ITU) X.500 provides directory services that may be used by users or host applications to locate other users and resources on the network. X.500 also provides security services used by DMS-compliant X.400 implementations. See section 6 for security standards. Since X.500 is not an internet standard, see 3.2.1.1.2.2 for operation over Internet Protocol (IP) based networks. The following standard is mandated:

- ITU-T X.500, The Directory - Overview of Concepts, Models, and Services - Data Communication Networks Directory, 1993.

3.2.1.1.1.2.2 Domain Name System (DNS)

The DNS provides the service of translating between host names and IP addresses. DNS uses Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) as a transport service when used in conjunction with other services. The following standard is mandated:

- IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987.

3.2.1.1.1.3 File Transfer

Basic file transfer shall be accomplished using File Transfer Protocol (FTP). FTP provides a reliable, file transfer service for text or binary files. FTP uses TCP as a transport service. The following standard is mandated:

- IAB Standard 9/RFC-959, File Transfer Protocol, October 1985, with the following FTP commands mandated for reception: Store unique (STOU) and Abort (ABOR).

3.2.1.1.1.4 Remote Terminal

Basic remote terminal services shall be accomplished using Telecommunications Network (TELNET). TELNET provides a virtual terminal capability that allows a user to "log on" to a remote system as though the user's terminal was directly connected to the remote system. The following standard is mandated:

- IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983.

3.2.1.1.1.5 Network Management

Network management provides the capability to manage designated network(s). This includes the capability to control the network's topology, dynamically segment the network into multiple logical domains, maintain network routing tables, monitor the network load, and make routing adjustments to optimize throughput. Network management also provides the capability to review and publish network addresses of network objects; monitor the status of network objects; start, restart, reconfigure, or terminate network objects; and detect loss of network objects in order to support automated fault recovery. Hosts shall implement the Simple Network Management Protocol (SNMP) set of network management protocols. The following standards are mandated:

- IAB Standard 15/RFC-1157, Simple Network Management Protocol (SNMP), May 1990
- IAB Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990
- IAB Standard 17/RFC-1213, Management Information Base, March 1991.

3.2.1.1.1.6 Network Time

Network Time Protocol (NTP) provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet. The following standard is mandated:

- RFC-1305, Network Time Protocol (V3), April 9, 1992.

3.2.1.1.1.7 Bootstrap Protocol (BOOTP)

BOOTP assigns an IP address to workstations with no IP address. The following standards are mandated:

- RFC-951, Bootstrap Protocol, September 1, 1985
- RFC-1533, DHCP Options and BOOTP Vendor Extensions, October 8, 1993
- RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993.

3.2.1.1.1.8 Dynamic Host Configuration Protocol (DHCP)

DHCP provides an extension of BOOTP to support the passing of configuration information to Internet hosts. DHCP consists of two parts, a protocol for delivering host-specific configuration parameters from a DHCP server to a host, and a mechanism for automatically allocating IP addresses to hosts. The following standard is mandated:

- RFC-1541, Dynamic Host Configuration Protocol, October 27, 1993.

3.2.1.1.1.9 World Wide Web (WWW) Services

3.2.1.1.1.9.1 Hypertext Transfer Protocol (HTTP)

HTTP is used for search and retrieval within the WWW. HTTP uses TCP as a transport service. The following standard is mandated:

- RFC-1945, Hypertext Transfer Protocol -- HTTP/1.0, May 17, 1996.

3.2.1.1.1.9.2 Uniform Resource Locator (URL)

A URL specifies the location of and access methods for resources on an internet. The following standards are mandated:

- RFC-1738, Uniform Resource Locators, December 20, 1994
- RFC-1808, Relative Uniform Resource Locators, June 14, 1995.

3.2.1.1.1.10 Connectionless Data Transfer

Variable Message Format (VMF) messages shall use a connectionless application layer. The following standard is mandated:

- MIL-STD-2045-47001, Connectionless Data Transfer Application Layer Standard, July 27, 1995.

3.2.1.1.2 Transport Services

The transport services provide host-to-host communications capability for application support services. The following sections define the requirements for this service.

3.2.1.1.2.1 Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) over Internet Protocol (IP)

3.2.1.1.2.1.1 Transmission Control Protocol (TCP)

TCP provides a reliable connection-oriented transport service. The following standard is mandated:

- IAB Standard 7/RFC-793, Transmission Control Protocol, September 1981. In addition, TCP shall implement the PUSH flag and the Nagle Algorithm, as defined in IAB Standard 3.

3.2.1.1.2.1.2 User Datagram Protocol (UDP)

UDP provides an unacknowledged, connectionless, datagram transport service. The following standard is mandated:

- IAB Standard 6/RFC-768, User Datagram Protocol, August 1980.

3.2.1.1.2.1.3 Internet Protocol (IP)

IP is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. Two other protocols are considered integral parts of IP: the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers. The following standard is mandated:

- IAB Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol, September 1981. In addition, all implementations of IP must pass received Type-of-Service (TOS) values up to the transport layer. Furthermore, for hosts that transmit or receive multiaddressed datagrams over Combat Net Radio (CNR), the multiaddressed IP option field must be used. This is a military-unique option that is defined in MIL-STD-2045-14502-1A.

3.2.1.1.2.2 Open Systems Interconnection (OSI)/Internet Interworking Protocol

This protocol provides the interworking between Transport Protocol Class 0 (TP0) and TCP transport service necessary for OSI applications to operate over IP-based networks. The following standard is mandated:

- IAB Standard 35/RFC 1006, ISO Transport Service on top of the TCP, May 1978.

3.2.1.2 Video Teleconferencing (VTC) Standards

VTC terminals operating at data rates of 56-1920 kbps shall comply with the Industry Profile for Video Teleconferencing, VTC001. The purpose of the profile is to provide interoperability between VTC terminal equipment, both in point-to-point and multipoint configurations. This profile is based on the ITU-T H.320 and T.120 series of recommendations. VTC terminals operating at low bit rates (9.6-28.8 kbps) shall comply with ITU-T H.324. The following standards are mandated:

- VTC001, Industry Profile for Video Teleconferencing, Revision 1, April 25, 1995
- ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, March 19, 1996.

3.2.1.3 Facsimile Standards

3.2.1.3.1 Analog Facsimile Standard

Facsimile requirements for analog output shall comply with ITU-T Group 3 specifications. The following standards are mandated:

- TIA/EIA-465-A, Group 3 Facsimile Apparatus for Document Transmission, March 21, 1995
- TIA/EIA-466, Procedures for Document Facsimile Transmission, May 1981.

3.2.1.3.2 Digital Facsimile Standard

Digital facsimile terminals operating in tactical, high Bit Error Rate (BER) environments shall implement digital facsimile equipment standards for Type I and/or Type II mode. Also, facsimile transmissions requiring encryption, or interoperability with NATO countries, shall use the digital facsimile standard. The following standard is mandated:

- MIL-STD 188-161D, Interoperability and Performance Standards for Digital Facsimile Equipment, January 10, 1995.

3.2.1.4 Secondary Imagery Dissemination Standards

The Tactical Communications Protocol 2 (TACO2) is the communications component of the National Imagery Transmission Standard (NITFS) suite of standards used to disseminate secondary imagery. TACO2 shall be used over point-to-point tactical data links in high BER disadvantaged communications environments. TACO2 is used to transfer secondary imagery and related products where JTA transfer protocols in section 3.2.1.1.2 fail. TACO2 only applies to users having simplex and half duplex links as their only means of communications. MIL-HDBK-1300A, NITFS, provides guidance to implement various Technical Interface Specifications (TIS) to connect the TACO2 host to specific cryptographic equipment. The following standard is mandated:

- MIL-STD-2045-44500, National Imagery Transmission Format Standard (NITFS) Tactical Communications Protocol 2 (TACO2), June 18, 1993.

3.2.2 Network Standards

3.2.2.1 Router Standards

Routers are used to interconnect various subnetworks and end systems. Protocols necessary to provide this service are specified below. RFC-1812 is an umbrella standard that references other documents and corrects errors in some of the reference documents. In addition, some of the standards that were mandated for hosts in Section 3.2.1.1 also apply to routers. The following standards are mandated:

- RFC-1812, Requirements for IP Version 4 Routers, June 22, 1995
- IAB Standard 6/RFC-768, User Datagram Protocol, August 1980
- IAB Standard 7/RFC-793, Transmission Control Protocol, September 1981
- IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983
- IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987
- IAB Standard 15/RFC-1157, Simple Network Management Protocol, May 1990
- IAB Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990
- IAB Standard 17/RFC-1213, Management Information Base, March 1991
- RFC-951, Bootstrap Protocol, September 1, 1985
- RFC-1533, DHCP Options and BOOTP Vendor Extensions, October 8, 1993
- RFC-1541, DHCP, October 27, 1993
- RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993
- IAB Standard 33/RFC-1350, Trivial FTP (TFTP), July 1992, to be used for initialization only.

Security requirements are addressed in Section 6.

3.2.2.1.1 Internet Protocol (IP)

IP is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. IP was designed to interconnect heterogeneous networks and operates over a wide variety of networks. Two other protocols are considered integral parts of IP, the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP is used to provide error reporting, flow control, and route redirection. IGMP provides multicast extensions for hosts to report their group membership to multicast routers. The following standard is mandated:

- IAB Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112, Internet Protocol, September 1981.

In addition, all implementations of IP routers that transmit or receive multiaddressed datagrams over Combat Net Radio (CNR), must use the multiaddressed IP option field. This is a military unique option that is defined in MIL-STD-2045-14502-1A.

3.2.2.1.2 IP Routing

Routers exchange connectivity information with other routers to determine network connectivity and adapt to changes in the network. This enables routers to determine, on a dynamic basis, where to send IP packets.

3.2.2.1.2.1 Interior Routers

Routes within an autonomous system are considered local routes that are administered and advertised locally by means of an interior gateway protocol. Routers shall use the Open Shortest Path First (OSPF) V2 protocol for unicast interior gateway routing and Multicast OSPF (MOSPF) for multicast interior gateway routing. The following standards are mandated:

- RFC-1583, Open Shortest Path First Routing Version 2, March 23, 1994, for unicast routing
- RFC-1584, Multicast Extensions to OSPF, March 24, 1994, for multicast routing.

3.2.2.1.2.2. Exterior Routers

Exterior gateway protocols are used to specify routes between autonomous systems. Routers shall use the Border Gateway Protocol 4 (BGP-4) for exterior gateway routing. BGP-4 uses TCP as a transport service. The following standards are mandated:

- RFC-1771, Border Gateway Protocol 4, March 21, 1995
- RFC-1772, Application of BGP-4 In the Internet, March 21, 1995.

3.2.2.2 Subnetworks

3.2.2.2.1 Local Area Network (LAN) Access

While no specific LAN technology is mandated, the following is required for interoperability in a joint environment. This requires provision for a LAN interconnection. Ethernet, the common implementation of Carrier Sense Multiple Access with Collision Detection (CSMA/CD), is the most common LAN technology in use with TCP/IP. The hosts use a CSMA/CD scheme to control access to the transmission medium. The following standards are mandated as the minimum LAN requirements for operation in a joint task force:

- ISO/IEC 8802-3:1993, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 10BaseT Medium-Access Unit (MAU)
- IAB-Standard 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984
- IAB Standard 37/RFC-826, An Ethernet Address Resolution Protocol, November 1982.

3.2.2.2.2 Point to Point Standards

For full duplex, synchronous or asynchronous, point-to-point communication, the following standards are mandated:

- IAB Standard 51/RFC-1661/RFC-1662, Point-to-Point Protocol (PPP), July 1994
- RFC-1332, PPP Internet Protocol Control Protocol (IPCP), May 26, 1992
- RFC-1333, PPP Link Quality Monitoring, May 26, 1992
- RFC-1334, PPP Authentication Protocols, October 20, 1992
- RFC-1570, PPP Link Control Protocol (LCP) Extensions, January 11, 1994.

The serial line interface shall comply with one of the following mandated standards:

- EIA 232E, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991

- EIA 449, General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, February 1980. (This calls out EIA 422B and 423B.)
- EIA 530A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992 (This calls out EIA 422B and 423B.).

3.2.2.2.3 Combat Net Radio (CNR) Networking

CNRs are a family of radios that allow voice or data communications for mobile users. These radios provide a half-duplex, broadcast transmission media with potentially high BERs. The method by which IP packets are encapsulated and transmitted is specified in MIL-STD-188-220A. With the exception of High Frequency (HF) networks, MIL-STD-188-220A shall be used as the standard communications net access protocol for CNR networks. The following standard is mandated:

- MIL-STD-188-220A, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, July 27, 1995.

3.2.2.2.4 Integrated Services Digital Network (ISDN)

ISDN is an international standard used to support integrated voice and data over standard twisted-pair wire. ISDN defines a Basic Rate Interface (BRI) and Primary Rate Interface (PRI) to provide digital access to ISDN networks. These interfaces support both circuit-switched and packet-switched services. The following standards are mandated:

For BRI physical layer,

- ANSI T1.601, Telecommunications - Integrated Services Digital Network (ISDN) - Basic Access Interface for Use on Metallic loops for Application on the Network Side of the NT (Layer 1 Specification), 1992.

For PRI physical layer,

- ANSI T1.408, Telecommunications - Integrated Services Digital Network (ISDN) - Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1990.

For BRI and PRI data link layer,

- ITU-T Q.921, ISDN User-Network Interface - Data Link Layer Specification - Digital Subscriber Signaling System No. 1, 1993.

For signaling at the user-network interface,

- ITU-T Q.931, ISDN User-Network Interface Layer 3 Specification for basic Call Control - Digital Subscriber Signaling System No. 1(DSS 1), Network Layer, User-Network Management, 1989.

For addressing,

- ITU-T E.164, Numbering Plan for the ISDN Era, 1991
- DCAC 370-175-13, Defense Switched Network System Interface Criteria, section titled Worldwide Numbering and Dialing Plan (WNDP), September 1993.

For transmitting IP packets when using ISDN packet-switched services,

- RFC-1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, August 6, 1992.

For transmitting IP packets using Point-to-Point Protocol (PPP) over ISDN,

- RFC-1618, PPP over ISDN, May 13, 1994.

The citation of applicable ANSI standards for ISDN does not assure C4I interoperability in regions outside North America where standards for these services differ. The JTA recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version.

3.2.2.2.5 Asynchronous Transfer Mode (ATM)

ATM is a high-speed switching technology that takes advantage of low BER transmission facilities to accommodate intelligent multiplexing of voice, data, video, imagery, and composite inputs over high-speed trunks. The network access protocols to connect user equipment to ATM switches are defined in the ATM Forum's User-Network Interface (UNI) Specification.

The protocol layers consist of an ATM Adaptation Layer (AAL), the ATM layer, and a physical layer. The role of AAL is to divide the variable-length data units into 48-octet units to pass to the ATM layer. AAL1 shall be used to support constant bit rate service, which is sensitive to cell delay, but not cell loss. AAL5 shall be used to support variable bit rate service. The following standards are mandated:

- ATM Forum's UNI Specification V 3.1, User-Network Interface, September 1994
- ANSI T1.630 ATM Adaptation Layer for Constant Bit Rate Services Functionality and Specification, 1993
- ANSI T1.635 ATM Adaptation Layer Type 5 Common Part Functions and Specifications, 1994, which adopts ITU-T I.363, section 6
- RFC-1577, Classical IP and Address Resolution Protocol (ARP) over ATM, January 20, 1994.

3.2.3 Transmission Media

3.2.3.1 Military Satellite Communications (MILSATCOM)

MILSATCOM systems include those systems owned or leased and operated by the DoD and those commercial SATCOM services used by the DoD. The basic elements of satellite communications consists of a space segment, control segment, and a terminal segment (air, ship, ground, etc.). An implementation of a typical satellite link will require the use of satellite terminals, user communications extension, and the use of military or commercial satellite resources.

3.2.3.1.1 Ultra High Frequency (UHF) Satellite Terminal Standards

3.2.3.1.1.1 5- and 25-kHz Service

For 5-kHz or 25-kHz single channel access service supporting the transmission of either voice or data, the following standard is mandated:

- MIL-STD-188-181, Interoperability Standard for Dedicated 5-kHz and 25-kHz UHF Satellite Communications, 18 September 1992.

3.2.3.1.1.2 5-kHz Demand Assigned Multiple Access (DAMA) Service

For 5-kHz DAMA service, supporting the transmission of data at 75 - 2400 bps and digitized voice at 2400 bps, the following standard is mandated:

- MIL-STD-188-182, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, 18 September 1992.

3.2.3.1.1.3 25-kHz Time Division Multiple Access (TDMA)/Demand Assigned Multiple Access (DAMA) Service

For 25-kHz TDMA/DAMA service, supporting the transmission of voice 2400, 4800, or 16000 bps and data at rates of 75 - 16000 bps, the following standard is mandated:

- MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992.

3.2.3.1.1.4 Data Control Waveform

For interoperable waveform for data controllers used to operate over single access 5 kHz and 25 kHz UHF SATCOM channels, the following standard (a robust link protocol that can transfer error free data efficiently and effectively over channels that have high error rates) is mandated:

- MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993.

3.2.3.1.2 Super High Frequency (SHF) Satellite Terminal Standards

3.2.3.1.2.1 Earth Terminals

For minimum mandatory Radio Frequency (RF) and Intermediate Frequency (IF) requirements to ensure interoperability of SATCOM earth terminals operating over C, X, and Ku- band channels, the following standard is mandated:

- MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995.

3.2.3.1.2.2 Phase Shift Keying (PSK) Modems

For minimum mandatory requirements to ensure interoperability of PSK modems operating in Frequency Division Multiple Access mode, the following standard is mandated:

- MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), January 13, 1995.

3.2.3.1.3 Extremely High Frequency (EHF) Satellite Payload and Terminal Standards

3.2.3.1.3.1 Low Data Rate (LDR)

For waveform, signal processing, and protocol requirements for acquisition, access control, and communications for low data rate (75 - 2400 bps) EHF satellite data links, the following standard is mandated:

- MIL-STD-1582, EHF LDR Uplinks and Downlinks, December 10, 1992.

3.2.3.1.3.2 Medium Data Rate (MDR)

For waveform, signal processing, and protocol requirements for acquisition, access control, and communications for medium data rate (4.8 kbps - 1.544 Mbits/s) EHF satellite data links, the following standard is mandated:

- MIL-STD-188-136, EHF MDR Uplinks and Downlinks, August 26, 1995.

3.2.3.2 Radio Communications

3.2.3.2.1 High Frequency (HF)

3.2.3.2.1.1 Automated Link Establishment (ALE)

For both ALE and radio subsystem requirements operating in the HF bands, the following standard is mandated:

- MIL-STD-188-141A, Medium and High Frequency Radio Equipment Standard, September 10, 1993.

3.2.3.2.1.2 Anti-jamming Capability

For anti-jamming capabilities for HF radio equipment, the following standard is mandated:

- MIL-STD-188-148, Interoperability Standard Anti-Jam Communications (2-30 Mhz), April 13, 1992.

3.2.3.2.1.3 Data Modems

For HF data modem interfaces, the following standard is mandated:

- MIL-STD-188-110A, Data Modems, Interoperability and Performance Standards, September 30, 1991.

3.2.3.2.2 Very High Frequency (VHF)

For radio subsystem requirements operating in the VHF frequency bands, the following standard is mandated:

- MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, June 20, 1985.

3.2.3.2.3 Ultra High Frequency (UHF)

For radio subsystem requirements operating in the UHF frequency bands, the following standard is mandated:

- MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, March 15, 1989.

3.2.3.2.4 Super High Frequency (SHF)

For radio subsystem requirements operating in the SHF frequency bands, the following standard is mandated:

- MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, July 28, 1992.

3.2.3.2.5 JTIDS/MIDS Transmission Media

For communicating with the JTIDS/MIDS radios the following standards are mandated:

- JTIDS System Segment Specification (Class 2 Terminal)-
- STANAG 4175, Edition 1, 29 August 1991 - Technical Characteristics of the Multifunctional Information Distribution System (MIDS)

3.2.3.3 Synchronous Optical Network (SONET) Transmission Facilities

The Synchronous Optical Network (SONET) is a telecommunications transmission standard for use over fiber-optic cable. SONET is the North American subset of the ITU standardized interfaces, and includes a hierarchical multiple structure, optical parameters, and service mapping. The following standards are mandated:

- ANSI T1.105, Telecommunications - Synchronous Optical Network (SONET) Basic Description Including Multiplex Structure, Rates and Formats (ATIS) (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991), 1995
- ANSI T1.107 Digital Hierarchy - Formats Specifications, 1995
- ANSI T1.117, Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991.

The citation of applicable ANSI standards for SONET does not assure C4I interoperability in regions outside North America where standards for these services differ. The JTA recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version.

3.3 EMERGING STANDARDS

The standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

3.3.1 Information Transfer Standards

Commercial communications standards and products will evolve over time. The JTA must evolve, as well, to benefit from these standards and products. The purpose of this section is to provide notice of those standards that are not yet a part of the JTA, but are expected to be adopted in the near future.

3.3.2 End System Standards

3.3.2.1 Internet Standards

IP Next Generation/Version 6 (IPv6). IPv6 is being designed to provide better internetworking capabilities than are currently available within IP (Version 4). IPv6 will include support for:

1. Expanded addressing and routing capabilities
2. A simplified header format
3. Extension headers and options
4. Authentication and privacy
5. Autoconfiguration
6. Simple and flexible transition to IPv6
7. Increased quality of service capabilities.

IP Version 6 is described in RFC-1883, IPv6 Specification, RFC-1884, IPv6 Addressing Architecture: RFC-1885, ICMPv6 for IPv6, and RFC-1886, DNS Extensions to support IPv6.

Mobile Host Protocol (MHP). The primary aim of MHP is to provide information reachability for the mobile host. The intent is that a mobile host should not have to perform any special actions because of host migration. A mobile IP protocol is currently available as an Internet draft, entitled IP Mobility Support.

3.3.2.2 Video Teleconferencing (VTC) Standards

There are two emerging VTC standards that support communications over different networks. ITU H.321 and ITU H.323 are draft recommendations that support VTC over ATM and Ethernet networks, respectively.

3.3.2.3 Global Positioning System (GPS)

GPS User Equipment must employ Precise Position Service (PPS) user equipment incorporating both Selective Availability and Anti-Spoofing features to support combat operations. The GPS guidelines that are documented in ASD Command, Control, Communications, and Intelligence (C3I) Memorandum "Development, Procurement, and Employment of DoD Global Position System, User Equipment," dated 31 April 1992 must be followed. Specific standards are being researched at this time.

3.3.3 Network Standards

3.3.3.1 Network Access Protocols

Wireless LAN. The IEEE 802.11 Committee is developing standards for wireless services across three transmission media: spread-spectrum radio; narrowband radio; and infrared energy. Wireless technology is useful in environments requiring mobility of the users or flexible network establishment and reconfiguration.

Fast Ethernet. For high speed requirements, 100 Mbits/s ethernet technology may be implemented in accordance with IEEE 802.3u. This standard supports auto-negotiation of the media speed, making it possible for dual-speed ethernet interfaces to run at either 10 or 100 Mbits/s automatically.

ATM-related Standards. The ATM Forum is developing Private Network-Network Interface (PN-NI) routing and signaling standards to support large, dynamic, multivendor ATM networks. PN-NI routing

will automatically disseminate network topology and resource information to switches in the network, enabling quality-of-service sensitive routing. Using this information, PN-NI signaling will allow calls to traverse large, dynamic networks in a scalable fashion. LANs, such as Ethernet, can be emulated over ATM networks using ATM LAN Emulation, Version 1.0. This permits ATM networks to be deployed without disruption of end-system network protocols and applications.

Personal Communications Services (PCS). PCS will support both terminal mobility and personal mobility. Personal mobility allows users of telecommunication services to gain access to these services from any convenient terminal with which they choose to associate themselves. To support personal mobility, the network must be able to distinguish between terminal and personal identifiers; to keep track of current user-terminal associations, user locations, services authorized to the user, and service capabilities of the terminals. Personal mobility may be provided by either wireline or wireless terminals. Terminal mobility is based on wireless access to the public switched telephone networks (PSTN). Wireless access standards will govern the protocols and procedures for establishing connections among mobile terminals and between them and fixed terminals of a switched network (or mobile terminals of a different cellular system). IS-41, the current standard within the United States, provides this capability and is compatible with the existing signaling and numbering schemes used in the PSTN.

Mobile Cellular. Mobile cellular radio can be regarded as an early form of "personal communications service." It allows subscribers to place and receive telephone calls over the PSTN wherever cellular service is provided. Two methods for digital access have emerged, TDMA, and Code Division Multiple Access (CDMA). In North America the standards for TDMA and CDMA are IS-54 and IS-95. Both of these standards use IS-41 as the standard signaling protocol.

Future Public Land Mobile Telecommunications Systems (FPLMTS) standards. The ITU is now working on a third-generation standard for FPLMTS. The aim of this effort is to achieve better compatibility among the various cellular systems such that, by the beginning of the next century, universal global access supporting terminal mobility becomes a reality. The document now emerging from this effort shall be used as guidance for implementing global terminal mobility.

3.3.3.2 Link 22 Transmission Standards

Link 22 Transmission media will be used to exchange Link 22 messages. Link 22 messages, comprised of F-Series formats, will be used for the exchange of maritime operational data between tactical data systems using line of sight (UHF) and beyond line of sight (HF) bands. The standard for Link 22 waveform is under development.

3.3.4 Military Satellite Communications (MILSATCOM)

Work is continuing on standards for MILSATCOM beyond the standards identified in section 3.2.3.1. The draft standards are:

1. MIL-STD-188-166 (Interface Standard, Interoperability and Performance of Non-Electronic Protective Measures (EPM) for SHF SATCOM Link Control Protocols and Messaging Standards)
2. MIL-STD-188-167 (Interface Standard, Message Format for SHF SATCOM Demand Assignment)
3. MIL-STD-188-168 (Interface Standard, Interoperability and Performance Standards for SHF Satellite Communications Mulitplexers and Demultiplexers)
4. MIL-STD-188-185 (Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System).

JTA SECTION 4 - INFORMATION MODELING AND INFORMATION STANDARDS

4.1 INTRODUCTION

4.1.1 Purpose

This section identifies the minimum standards applicable to information modeling and exchange of information for all DoD programs. Information standards pertain to activity models, data models, data definitions, and information exchanges among systems.

4.1.2 Scope

This section provides a set of standards affecting the definition, design, development, and testing of information models and information exchange among systems. It is applicable at all organizational levels and environments, including tactical, strategic, and interfaces to weapons systems. This section addresses information modeling and information standards. Information modeling mandates apply to all systems or components of systems. Information standards mandates apply to all information systems which must interact with any external system or device.

The relationship of Information Models to the DoD Technical Reference Models (TRM) is illustrated in Figure 4-1 . Activity models identify functionality required of mission area applications and identify the types of information required in the data model to support the mission area function. The information requirements identified in the activity model shall be used as the basis for developing a fully attributed, application-specific data model. The data model identifies the logical information requirements and metadata, which forms a basis for physical database schemata and standard data elements. Once implemented in operational systems, the data will be shared using generic information exchange standards.

An information model is a representation at one or more levels of abstraction of a set of real-world processes, products, and/or interfaces. Within the Information System (IS) domain, there are three basic types of models frequently created: activity, data, and interface. Activity models are representations of mission area applications, composed of one or more related activities. Information required to support the mission area function is the primary product of each activity model. A data model, developed from the information requirements documented in the activity model, define entities and their data elements and illustrate the interrelationships among the entities. Interface models tie disparate activities/processes together for a combined functionality. Interface models are customized to fit a particular project, hence material developers and system engineers should create and use interface models as necessary. Security standards related to this section are in Section 6.2.4. This section focuses on the use of data and activity models.

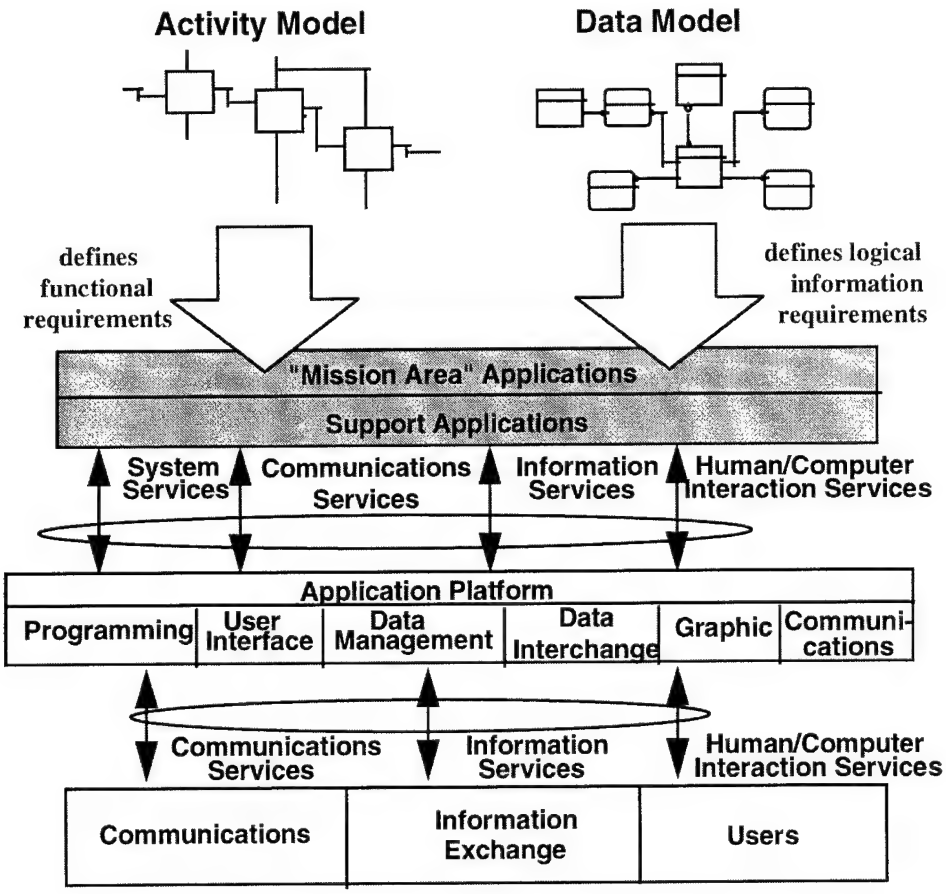


Figure 4-1. Relationship of Information Models to the DoD Technical Reference Model

To support the identification of information and information interchange requirements, the DoD has adopted the Federal Information Processing Standards (FIPS) Publication 183, Integration Definition for Function Modeling (IDEF0) and FIPS Publication 184, Integration Definition for Information Modeling (IDEF1X), for activity and data modeling, respectively. The Integrated (Computer-Aided Manufacturing) Definition (IDEF) Modeling methodology defines an unambiguous set of the following components:

a.) Symbols (i.e., syntax) associated with modeling concepts and ideas
b.) Rules for composing these symbols into abstract constructs
c.) Rules for mapping "meanings" (i.e., semantics) to these constructs
d.) Definitions of the relationships between activities and entities.

Information Standards define a logical view of data (meaning and contextual use) within an architecture. The activity model is a view of the activities, both automated and manual, that an organization must perform to achieve its mission. Modeling an organization's processes and data begins at the highest logical level, decomposes into lower logical levels and is communicated in a format that the users, particularly the subject matter experts, can easily understand and use.

In order to provide a single authoritative source for data standards, the DoD created the Defense Data Dictionary System (DDDS). The DDDS, managed by DISA, is a DoD-wide central database that includes standard data entities, data elements, and access to data models. The DDDS is used to collect individual

data standards derived from the DoD data model and to document content and format for data elements. The DDDS is the authoritative source for all DoD data standards.

Recent studies show three necessary data characteristics must be known to define interoperable databases. First, the contextual view of data must be developed to understand how data elements interact with each other. Second, the data element definitions must be unambiguous. Third, the foreign key identifiers must be defined in parent-to-child data relationships. These characteristics are contained within the combination of the DDDS, IDEF0, and IDEF1X models. Figure 4-2 provides a logical view of how the activity and data modeling standards contained in this section will support the development of interoperable systems.

Today, Command, Control, Communications, Computers, and Intelligence (C4I) information exchange is accomplished for the most part by sending fixed content formatted messages. The definition and documentation of these exchange mechanisms are provided by various messaging standards. Each message standard provides a means to define message form and functions (i.e., transfer syntax), which includes the definition of the message elements that are contained in each message. The message fields, which are currently defined in the various message standards, are not necessarily mutually consistent, nor are they consistently based on any process or data models either within a message system or across message systems. Newer techniques provide direct database-to-database exchange of data without the user following a rigid format. A model based on structure will eventually provide definitions which will be data elements-based and will be compliant with the defense data element standards established in accordance with the DoD Directive (DoDD) 8320.1, Data Administration, and associated DoD 8320.1 manuals.

4.1.3 Background

C4I is the framework for situational awareness, decision making, and execution throughout the battlespace. Efficient execution of information exchange requirements (IERs) throughout the joint battlespace is key to evolving C4I toward the ultimate goal of seamless information exchange. The primary component of this infrastructure is the C4I Tactical Data Link (TDL), comprised of message elements/messages and physical media. However, due to the diversity of Warfighter requirements, no single data link is applicable to every C4I platform and weapon system.

Tactical Digital Information Links (TADILs), structured on bit-oriented message standards, evolved to meet critical real-time and near-real-time message requirements. The United States Message Text Format (USMTF), designed primarily for non-real-time exchange, is based on a character-oriented message format and is the standard for man-readable and machine-processable information exchange. TDLs, character-oriented/man-readable (USMTF messages), imagery standards, voice, and video will provide a timely, integrated, and coherent picture for joint commanders and their operational forces.

Disparate data link message formats and communications media have resulted in untimely delivery of crucial battlefield information. This causes significant interoperability problems among the Commanders-in-Chief (CINCs), Services, Agencies (C/S/As), and allied nations. Currently, it is difficult to establish seamless information flow among diverse data link units. Future joint operations, such as ballistic missile defense and battlefield digitization, will place greater emphasis on the need for automated C4I functions. Tomorrow's battlefields will vastly increase the burden on C4I networks.

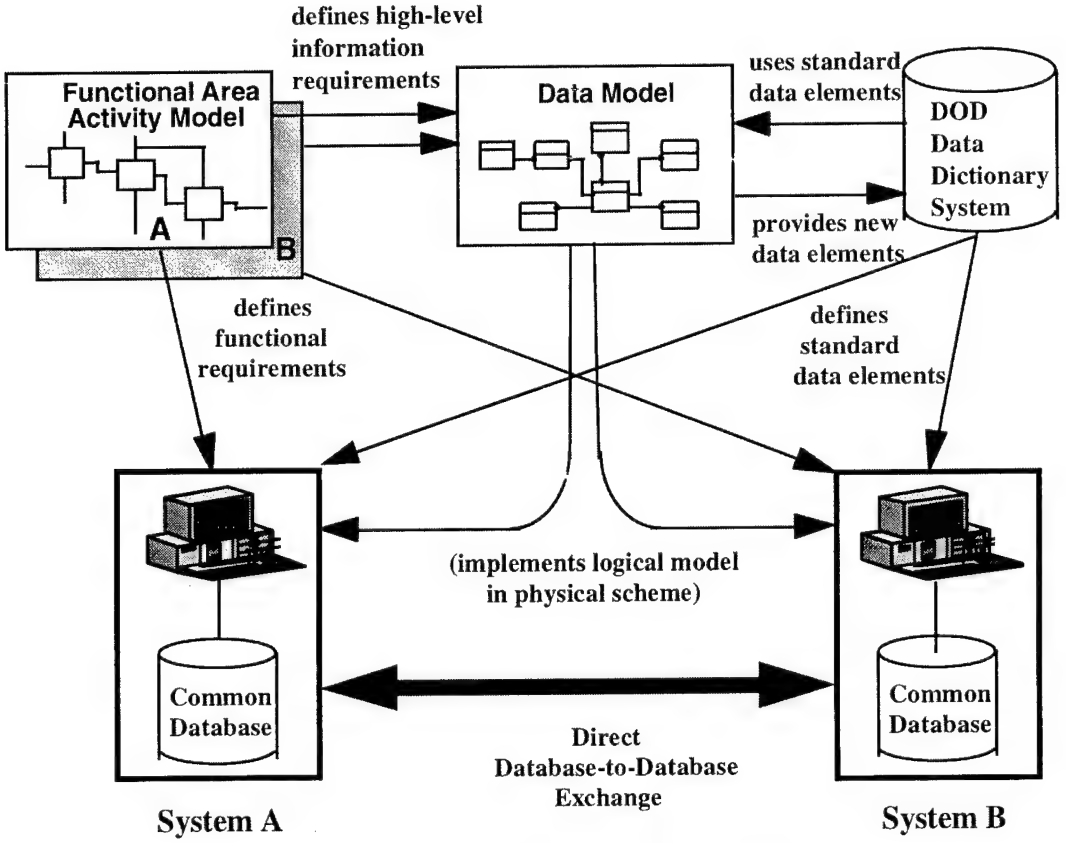


Figure 4-2. Objective Information Standards TA

4.2 MANDATES

This subsection identifies the mandatory standards, profiles, and practices for information modeling and information standards. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards. The World Wide Web (WWW) version of Appendix B contains a link to the standard or to the organization that maintains the standard when one is available.

4.2.1 Activity Model

Activity models are used to document/model the activities, processes, and data flows supporting the requirements of a new system or a major update. Prior to system development, an activity model is prepared to depict the mission area function to a level of detail sufficient to identify each entity in the data model that is involved in an activity. The activity model forms the basis for data model development or refinement. The activity model is validated against the requirements and doctrine, and approved by the operational sponsor.

The mandated standard for activity modeling is:

- FIPS PUB 183, Integration Definition for Function Modeling (IDEF0).

4.2.2 Data Model

The DoD Data Model (DDM) is a department-wide data model which provides the standard definition and use of specific data elements to the developers of all DoD systems. Adherence to the DDM will ensure DoD agencies are data interoperable among all information systems. The information requirements of a new or major system shall be documented within a data model. The basis for data modeling shall be DDM.

Tactical systems shall incorporate applicable Command and Control (C2) Core Data Model (C2CDM) requirements. The C2CDM is a subset of the DDM. Both are accessible via File Transfer Protocol (FTP) from the DDDS server. The DDM provides the tactical metadata and modeling elements for all approved, candidate, and developmental DoD data standards managed by the functional data stewards. New information requirements are submitted by requiring Components and Defense Agencies and approved by functional data stewards in accordance with DoD Manual 8320.1-M-1, DoD Data Standardization Procedures and shall be used to extend the DDM and C2CDM, as appropriate. Computer Automated Software Engineering (CASE) tools that support IDEF1X diagrams are used to extend the model with additional logical entities, attributes, and relationships.

The data models shall be used in software requirements analyses and design activities as a logical basis for physical database design. Developers of new and existing systems shall maintain traceability between their physical database schema and the DDM and C2CDM, as applicable, allowing links from interface requirements to database population and update processes. The Intelligence community's Modernized Integrated Database (MIDB) is being harmonized with the C2CDM and migrating to DDM.

The mandated standards for Data Modeling are:

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures
- FIPS PUB 184, Integration Definition For Information Modeling (IDEF1X). December 1993.

4.2.3 DoD Data Definitions

The Defense Data Dictionary System (DDDS) is a central database that includes standard data entities, data elements, and provides access to DDM files from the DDDS server. Procedures governing the use of and access to the DDDS are delineated in DoD Manual 8320.1-M-1. A classified version of the DDDS, known as the Secure Intelligence Data Repository (SIDR), is being developed to support standardization of classified data elements and domains. System developers shall use the DDDS as a primary source of data element standards.

The mandated standards for DoD Data Definitions are:

- DoD Manual 8320.1-M-1, DoD Data Standardization Procedures
- Defense Data Dictionary System (DDDS).

4.2.4 Information Standards

4.2.4.1 Information Standards Applicability

Information Standards refer to the exchange of information among mission area applications within the same system or among different systems. The scope of information standards. follows:

- The exchange of information among applications shall be based on the logical data models developed from identifying information requirements through activity models, where appropriate. The data model identifies the logical information requirements, which shall be developed into physical database schemata and standard data elements.

- The standard data elements shall be exchanged using the data management, data interchange, and distributed computing services of application platforms. (Refer to Section 2 for further guidance on these services.) The goal is to exchange information directly between information systems, subject to security classification considerations.
- System information exchange shall satisfy the doctrinally operational Information Standards Requirements that have been developed and approved for the systems.

For purposes of clarification, Information Standards is the system or application-independent ability of data to be shared, whereas Data Interchange is system or application-specific. Hence, this section discusses information standards as the generic ability of a system or application to share data. Interchange standards help form the Common Operating Environment (COE) ensuring the use of system or application formats which can share data. Key references include Section 2.2.2.1.3, for SQL standards in Data Management Services and Section 2.2.2.1.4 for Data Interchange Services.

The message standards below are joint/combined message standards that provide for the formatted transfer of information between systems. Although it must be recognized that the J-Series Family of TDLs and the USMTF Standards are not model-based and therefore do not meet the goals of standard information exchange, they must be recognized as existing standards. As more systems are developed using logical data models and standard data elements, these message standards must evolve to be data model-based if they are to continue to support joint automated systems.

4.2.4.2 Tactical Information Standards

4.2.4.2.1 Bit-Oriented Data

The J-Series Family of TDLs allow information exchange using common data element structures and message formats which support time critical information. They include Air Operations/Defense Maritime, Fire Support, and Maneuver Operations. These are the primary data links for exchange of bit-oriented information. The family consists of LINK 16, LINK 22, and the Variable Message Format (VMF) and interoperability is achieved through use of J-Series family messages and data elements. The policy and management of this family is described in the Joint Tactical Data Link Management Plan (JTDLMP), dated April 1996.

New message requirements shall use these messages and data elements or use the message construction hierarchy described in the JTDLMP. The mandated standards for information exchange are:

- JTIDS Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 3 August 1994
- STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 2 March 1990
- VMF Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 1 February 1995.

4.2.4.2.2 US Message Text Format (USMTF) Messages

USMTF messages are jointly agreed, fixed-format, character-oriented messages that are man-readable and machine-processable. The standard is documented in MIL-STD 6040 and the interface operating procedures are documented in CJCSM 6120.05, Procedures for US Message Text Formats. USMTFs are the mandatory standard for record AUTODIN and in the future, DMS messages when communicating with the Joint Staff, Combatant Commands, and Service Components.

The mandated standard for USMTF Messages is:

- MIL-STD-6040, United States Message Text Format (USMTF).

4.2.4.2.3. Database-to-Database Exchange

The distributed computing services stated in Section 2.2.2.2.4 provide the capability to exchange standard data among heterogeneous platforms.

The following is mandated:

- Database-to-Database Exchange shall use standard data elements from DDDS.

4.3 EMERGING STANDARDS

The standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

4.3.1 Activity Model

There are no emerging activity models standards.

4.3.2 Data Modeling

The emerging standard for data modeling is IDEF1X97, Conceptual Schema Modeling. This standard accommodates object-oriented methods (OOM). IDEF1X97 is being developed by the IEEE IDEF1X Standards Working Group of the IEEE 1320.2 Standards Committee. The standard describes two styles of the IDEF1X model. The *key-style* is used to produce information models which represent the structure and semantics of data within an enterprise and is backward-compatible with the US Government's Federal Standard for IDEF1X, FIPS 184. The *identity-style* is a wholly new language which provides system designers and developers a robust set of modeling capabilities covering all static and many dynamic aspects of the emerging object model. This identity-style can, with suitable automation support, be used to develop a model which is an executable prototype of the target object-oriented system. The identity-style can be used in conjunction with emerging dynamic modeling techniques to produce full object-oriented models.

4.3.3 DoD Data Definitions

DISA JIEO, in coordination with the Standards Coordinating Committee (SCC) and the Change Control Board (CCB), will develop the strategy/policy for migration from many tactical data link (bit-oriented) and character-oriented joint message standards to a minimal family of DoD 8320.1-compliant information exchange standards. A normalized unified data/message element dictionary will be developed based on normalized Data Model and associated data element standards. The dictionary will support both character and bit-oriented representation of the standard data and their domain values. Message standards will then establish the syntax for standard data packaging to support mission requirements (e.g., character or bit-oriented, fixed or variable format, etc.). The unified data dictionary will ensure that multiple representations are minimized and transformation algorithms are standardized. The Data Model basis for the data elements will ensure the information is normalized. A classified version of the DDDS, known as the SIDR, is being developed to support standardization of classified data elements and domains.

4.3.4 Information Standards

JTIDS will soon be supplemented by the Multi-functional Information Distribution System (MIDS). Message format standards for MIDS will not change from those of the JTIDS. Message and data element standards must be independent of the information transfer standards, protocols, and profiles. Refer to section 3 of this document for information transfer standards.

MIL-STD-6016 will most likely be called DoD Interface Standard, Tactical Digital Information Link (TADIL) J Message Standard, expected to be dated on or about 30 September 1996.

STANAG 5516, Edition 2, is currently under development at JIEO, for delivery to the NATO Data Ling Working Group (DLWG) sometime prior to the 11th meeting in November 1996.

STANAG 5522, Edition 1, Tactical Data Exchange - LINK 22 (Undated) is the Configuration Management (CM) baseline document.

VMF Technical Interface Design Plan - Reissue 2, is currently under development at JIEO, with a planned release date by 30 August 1996.

JTA SECTION 5 - HUMAN-COMPUTER INTERFACES

5.1 INTRODUCTION

5.1.1 Purpose

This section provides a common framework for Human-Computer Interface (HCI) design and implementation in DoD Command, Control, Communications, Computers, and Intelligence (C4I) systems. The objective is to standardize user interface design and implementation options thus enabling DoD applications within a given domain to appear and behave consistently. The standardization of HCI appearance and behavior within the DoD will result in higher productivity, shorter training time, and reduced development, operation, and support costs.

This section focuses on one component (HCI style) of the user interface (UI). Other components, their services and interrelationships (interfaces) are required to address application interoperability and portability issues and requirements in the DoD UI space.

5.1.2 Scope

This section applies to all Command, Control, Communications, Computers, and Intelligence (C4I) Systems and the interfaces of those systems with other key assets (e.g., weapon systems, sensors, models and simulations) to support critical joint Warfighter interoperability. This section addresses the presentation and dialogue levels of the Human-Computer Interface. Section 2 addresses the application program interface definitions and protocols. See Section 6.2.5 and Appendix A, Security Presentation Guidelines, DoD HCI Style Guide, and other applicable portions of the DoD HCI Style Guide for HCI Security.

5.1.3 Background

The objective of system design is to ensure system reliability and effectiveness. To achieve this objective the human must be able to effectively interact with the system. Humans interact with automated systems using the HCI. The HCI includes the appearance and behavior of the interface, physical interaction devices, graphical interaction objects, and other human-computer interaction methods. A good HCI is both easy to use and appropriate to the operational environment. It exhibits a combination of user-oriented characteristics such as intuitive operation, ease and retention of learning, facilitation of user task performance, and consistency with user expectations.

The need to learn the appearance and behavior of different HCIs used by different applications and systems increases both the training burden and the probability of operator error. What is required are interfaces that exhibit a consistent appearance and behavior both within and across applications and systems.

An HCI style guide is a document that specifies design rules and guidelines for the look and behavior of the user interaction with a software application or a family of software applications. The goal of a style guide is to improve human performance and reduce training requirements by ensuring consistent and usable design of the HCI across software modules, applications, and systems. The style guide represents "what" user interfaces should do in terms of appearance and behavior, and can be used to derive HCI design specifications which define "how" the rules are implemented in the HCI application code.

5.2 MANDATES

This subsection identifies the mandatory standards, profiles, and practices for human-computer interfaces. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards. The World Wide Web (WWW) version of Appendix B contains a link to the standard or to the organization that maintains the standard when one is available.

5.2.1 General

The predominant types of HCIs include graphical user interfaces (GUIs) and character-based interfaces. For all DoD automated systems, the near-term goal is to convert character-based interfaces to GUIs. Although GUIs are the preferred user interface, some specialized interfaces (e.g., hand-held device) may require use of character-based or alternative interfaces due to operational, technical, or physical constraints. These specialized interfaces shall be defined by domain-level style guides and further detailed in system-level user interface specifications. In order to present a consistent interface to the user, graphical and character-based interface styles should not be mixed within the same system.

The following is mandated for systems with an approved requirement for a character-based interface:

- DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September, 1994.

While not mandated, additional guidance for developing character-based interfaces can be found in ESD-TR-86-278, Guidelines for Designing User Interface Software (Smith and Mosier 1986).

When developing DoD automated systems, the graphical user interface shall be based on one commercial user interface style guide consistent with Section 5.2.2.1. Hybrid GUIs that mix user interface styles (e.g., Motif with Windows) shall not be created. A hybrid GUI is a GUI that is composed of toolkit components from more than one user interface style. When selecting commercial off-the-shelf (COTS)/government off-the-shelf (GOTS) applications for integration with developed DoD automated systems, maintaining consistency in the user interface style is highly recommended.

5.2.2 Style Guides

Figure 5-1 illustrates the hierarchy of style guides that shall be followed to maintain consistency and good HCI design within the DoD. This hierarchy, when applied according to the process mandated in the DoD HCI Style Guide, provides a framework that supports iterative prototype-based HCI development. The process starts with top-level general guidance and uses prototyping activities to develop system-specific design rules.

The interface developer shall use the selected commercial GUI style guide, refinements provided in the DoD HCI Style Guide, and the appropriate domain-level style guide for specific style decisions along with input of human factors specialists to create the system-specific HCI. The following paragraphs include specific guidance regarding the style guide hierarchy levels.

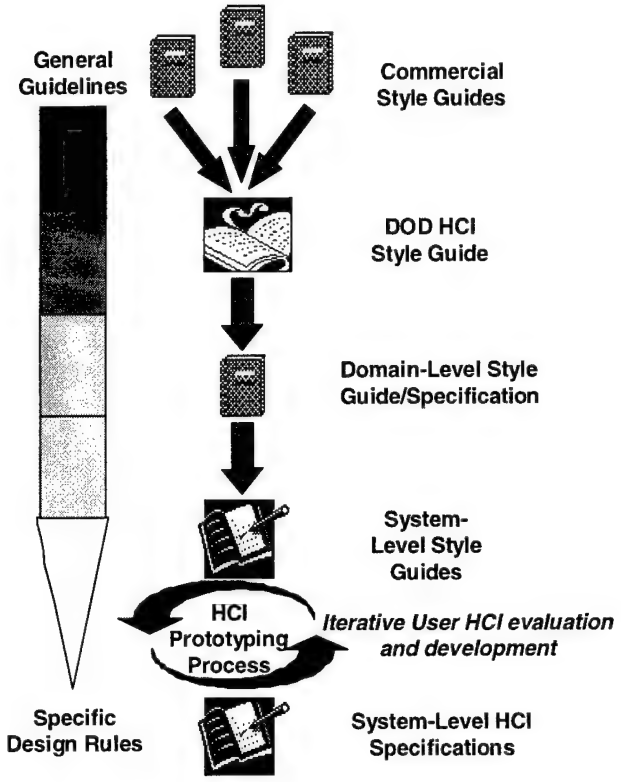


Figure 5-1. HCI Development Guidance

5.2.2.1 Commercial Style Guides

A commercial GUI style shall be selected as the basis for user interface development. The GUI style selected is usually driven by the mandates specified in Section 2 (User Interface Services and Operating System Services).

If Motif based environment is selected, the following is mandated:

- Open Software Foundation (OSF)/Motif™ Style Guide, Revision 1.2 (OSF 1992).

If Windows based environment is selected, the following is mandated:

- The Windows™ Interface: An Application Design Guide, Microsoft Press, 1992.

5.2.2.2 DoD Human-Computer Interface (HCI) Style Guide

The DoD HCI Style Guide is a high level document which allows consistency across DoD systems without undue constraint on domain and system level implementation. The DoD HCI Style Guide (Volume 8 of the TAFIM) was developed as a guideline document presenting recommendations for good Human-Computer Interface design. This document focuses on Human-Computer behavior and concentrates on elements or functional areas that apply to DoD applications. These functional areas include such things as security classification display, mapping display and manipulation, decision aids, and embedded training. This style guide, while emphasizing commercial GUIs, contains guidance that can be used for

all types of systems including those which employ character-based interfaces. Although the DoD HCI Style Guide is not intended to be strictly a compliance document, it does represent DoD policy.

The following guideline is mandated:

- DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September, 1994.

Although the general principles given in this document apply to all interfaces, some specialized areas require separate consideration. Specialized interfaces, such as those used in hand-held devices, have interface requirements that are beyond the scope of the DoD HCI Style Guide. These systems shall comply with their domain-level style guide and follow the general principles and HCI design guidelines presented in the DoD HCI Style Guide.

5.2.2.3 Domain-level Style Guides

The Joint Technical Architecture (JTA) mandates the development of a domain-level HCI style guide for each approved domain within the DoD. These style guides will reflect the consensus on HCI appearance and behavior for a particular domain (e.g., C4I) within the DoD. The domain-level style guide will be the compliance document and may be supplemented by a system-level style guide.

The following domain-level style guide is mandated for Motif based C4I systems.

- User Interface Specification for the Defense Information Infrastructure (DII), June 1996

5.2.2.4 System-level Style Guides

System-level style guides provide the special tailoring of commercial, DoD, and domain-level style guides. These documents include explicit design guidance and rules for the system, while maintaining the appearance and behavior provided in the domain-level style guide. If needed, the Motif based C4I system-level style guide will be created in accordance with the User Interface Specification for the DII.

5.3 EMERGING STANDARDS

The standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

MIL-STD-2525 Version 1 is an interim standard scheduled to be superseded by MIL-STD-2525A in late 1996. This standard provides common warfighting symbology along with details on its display and plotting to ensure the compatibility and interoperability of C4I systems displays. MIL-STD 2525A is intended to correct significant deficiencies in Version 1 and it is anticipated that it will be mandated in future versions of the JTA.

Currently, research is underway to investigate non-traditional user interfaces. Such interfaces may be gesture-based and may involve processing multiple input sources, such as voice and spatial monitors. Ongoing research and investigation includes the use of virtual reality and interface agents. Interface agents autonomously act on behalf of the user to perform various functions, thus allowing the user to focus on the control of the task domain. The DoD will integrate standards for non-traditional user interfaces as research matures and commercial standards are developed.

CDENext Style Guide, a commercial style guide for the Common Desktop Environment (CDE) is projected to be released in late 1996. This style guide merges features of Motif 2.0 and the CDE version 1.0 with enhancements.

JTA SECTION 6 - INFORMATION SYSTEMS SECURITY STANDARDS

6.1 INTRODUCTION

6.1.1 Purpose

This section provides the information system security standards necessary to implement security at the required level of protection.

6.1.2 Scope

The standards mandated in this section apply to all Command, Control, Communications, Computers, and Intelligence (C4I) systems. This section provides the security standards applicable to information processing, transfer, modeling and standards, and Human-Computer Interfaces (HCI). This section also addresses standards for security audit and key management mechanisms. Subsection 6.2 addresses mandated security standards, and subsection 6.3 addresses emerging security standards.

6.1.3 Background

The Technical Architecture Framework for Information Management (TAFIM) provides a blueprint for the Defense Information Infrastructure (DII), capturing the evolving vision of a common, multipurpose, standards-based technical infrastructure. The DoD Goal Security Architecture (DGSA), Volume 6 of the TAFIM, provides a comprehensive view of the architecture from the security perspective. The DGSA is a generic architectural framework for developing mission specific security architectures which includes security services for information systems (authentication, access control, data integrity, data confidentiality, non-repudiation, and availability). Although advancements in security theory and technology are needed to develop DGSA-consistent systems, the DGSA concepts and principles can be incorporated into current systems.

Interoperability requires seamless information flow at all levels of information classification without compromising security. The goal is to protect information at multiple levels of security, recognizing that today's DoD systems are "islands" of system-high solutions.

Systems that process sensitive data must be certified and accredited before use. Certification is the technical evaluation of security features and other safeguards, made in support of the accreditation. Accreditation is the authorization by the Designated Approving Authority (DAA) that an information system may be placed into operation. By authorizing a system to be placed in operation, the DAA is declaring that the system is operating under an "acceptable level of risk." Therefore, system developers should open dialog with the Certifier and DAA concurrently with their use of the Joint Technical Architecture (JTA), as DAA decisions can affect the applicability of standards within specific environments.

DoD systems should have adequate safeguards to enforce DoD security policies and system security procedures. System safeguards should provide adequate protection from user attempts to circumvent system access control, accountability, or procedures for the purpose of performing unauthorized system operations.

Security requirements and engineering should be determined in the initial phases of design. The determination of security services to be used and the strength of the mechanisms providing the services

are primary aspects of developing the specific security architectures to support specific domains. Section 6 of the JTA is used after operational architectural decisions are made regarding the security services needed and the required strengths of protection of the mechanisms providing those services.

The proper selection of standards can also provide a basis for improved information protection. Although few specific standards for the general topic of "information protection" exist, within Defensive Information Warfare, selecting standards with security-relevant content contributes to the overall improvement of the security posture of information systems.

6.2 MANDATES

This subsection identifies the mandatory standards, profiles, and practices for information systems security standards. Each mandated standard or practice is clearly identified on a separate line, and includes a formal reference that can be included within Requests for Proposals (RFP) or Statements of Work (SOW). Appendix B contains a table that summarizes the mandated standards from this section, as well as providing information on how to obtain the standards. The WWW version of Appendix B contains a link to the standard or to the organization that maintains the standard when one is available.

6.2.1 Introduction

This section contains the mandatory information systems security standards and protocols that shall be implemented in systems that have a need for the corresponding interoperability-related services. If a service is to be implemented in a C4I system, then it shall be implemented at the required level of protection using the associated security standards in this section. If a service is provided by more than one standard, the appropriate standard should be selected based on system requirements.

6.2.2 Information Processing Security Standards

Technical evaluation criteria to support information system security policy, and evaluation and approval, disapproval, and accreditation responsibilities are promulgated by DoD Directive (DoDD) 5200.28. Based on the required level of trust, the following information processing security standards are mandated.

6.2.2.1 Application Software Entity Security Standards

The following standards are mandated for the development and acquisition of application software consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985
- NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991.

If FORTEZZA services are used, the following are mandated:

- FORTEZZA Application Implementors' Guide, MD4002101-1.52, 5 March 1996
- FORTEZZA Cryptologic InterfaceProgrammers' Guide, MD4000501-1.52, 30 January 1996.

6.2.2.2 Application Platform Entity Security Standards

For the application platform entity, security standards are mandated for data management services and operating system services.Security is an important part of other platform service areas, but there are no standards mandated.

6.2.2.2.1 Data Management Services

The following standard is mandated for data management services consistent with the required level of trust:

- NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991.

6.2.2.2.2 Operating System Services Security

For the application platform entity, the following standard is mandated for the acquisition of operating systems consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985.

6.2.2.2.2.1 Security Auditing and Alarms Standards

Security auditing is a review or examination of records and activities to test controls, ensure compliance with policies and procedures, detect breaches in security, and indicate changes in operation. Security alarm reporting is the capability to receive notifications of security-related events, alerts of any misoperations and security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security.

The following standard is mandated for security auditing or alarm reporting:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985

6.2.2.2.2.2 Authentication Security Standards

Authentication supports tracing security-relevant events to individual users. The following standard is mandated:

- FIPS PUB 112, Password Usage, NIST, 30 May 1985.

If Open Software Foundation (OSF) Distributed Computing Environment (DCE) Version 1.1 is used, the following authentication standard is mandated:

- RFC-1510, The Kerberos Network Authentication Service, V.5, 10 September 1993.

6.2.3 Information Transfer Security Standards

This section discusses the security standards that shall be used when implementing information transfer security services. Security standards are mandated for the following information transfer areas: end system (host standards), and network (internetworking standards).

6.2.3.1 End System Security Standards

Security standards for host end systems are included in the following subsections.

6.2.3.1.1 Host Security Standards

Host end system security standards include security algorithms, security protocols, and evaluation criteria. The first generation FORTEZZA Cryptographic Card and its successor the Type I Card (formerly known as FORTEZZA Plus) are designed for protection of information in messaging and other applications.

For systems required to interface with Defense Message System, the following standards are mandated:

- FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994
- FORTEZZA Plus Interface Control Document, Release 3.0, 1 June 1995.

6.2.3.1.1.1 Security Algorithms

To achieve interoperability, products must support a common transport protocol. Transport protocols must agree on a common cryptographic message syntax, cryptographic algorithms, and modes of operations (e.g., cipher block chaining). Transport protocols support negotiation mechanisms for selecting common syntax, algorithms, and modes of operation.

The following paragraphs identify security standards that shall be used for the identified types of cryptographic algorithms: message digest or hash, digital signature, encryption, and key exchange.

Message digest or hash algorithms are one-way functions which create a "fingerprint" of a message. They provide data integrity when used in conjunction with other cryptographic functions. If message digest or hash algorithms are required, the following standard is mandated:

- FIPS PUB 180-1, Secure Hash Standard, NIST, April 1995.

Digital signatures provide strong identification and authentication. Related standards include public key certificate standards (X.509) and directory service standards (X.500). If digital signature is required, the following standard is mandated:

- FIPS PUB 186, Digital Signature Standard, NIST, May 1994.

Encryption prevents unauthorized disclosure of information during transmission. Systems processing classified information must use a Type 1 NSA-approved encryption product, which can also be used to encrypt sensitive but unclassified information. To provide for lawful authorized access to the keys required to decipher enciphered information for systems requiring strong encryption protection of sensitive but unclassified information, the following standard is mandated:

- FIPS PUB 185, Escrowed Encryption Standard, NIST, 9 February 1994.

Key exchange algorithms allow two parties to exchange encryption keys without relying on out-of-band communications. In FORTEZZA applications, the following NSA-developed Type II key exchange algorithm is mandated:

- Key Exchange Algorithm, NSA, R21-TECH-23-94, 12 July 1994.

6.2.3.1.1.2 Security Protocols

The following standard is mandated for DoD systems that are required to exchange security attributes, for example sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 25 January 1995.

Establishment of a certificate and key management infrastructure for digital signature is required for the successful implementation of the security architecture. This infrastructure is responsible for the proper creation, distribution, and revocation of end users' public key certificates. The following standard is mandated:

- ITU-T Rec. X.509 (ISO/IEC 9594-8.2), Version 3, The Directory: Authentication Framework (1993).

MIL-STD-2045-18500 is based on Version 3.0 of the Message Security Protocol (MSP) documented in SDN 701, Secure Data Network System Message Security Protocol, Revision 1.5, 1 August, 1989. The following messaging protocol is mandated for DoD message systems that are required to exchange sensitive but unclassified and classified information:

- MIL-STD-2045-18500, Message Handling System Message Security Protocol (MSP) Profile, October 1993.

The following key management protocol is mandated:

- SDN.903, revision 3.2, Secure Data Network System (SDNS) Key Management Protocol (KMP), August 1, 1989.

6.2.3.1.1.3 Evaluation Criteria Security Standards

The following standards are mandated consistent with the required level of trust:

- DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985
- NCSC-TG-005, Version-1, Trusted Network Interpretation, July 1987.

6.2.3.2 Network Security Standards

Mandated network security standards are included in subsection 6.2.3.2.1.

6.2.3.2.1 Internetworking Security Standards

See subsection 6.2.3.1.1.1. When key escrow encryption is required, the following standard is mandated:

- FIPS PUB 185, Escrowed Encryption Standard, NIST, 9 February 1994.

When network layer security is required, the following security protocol is mandated:

- SDN.301, revision 1.5, Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989.

The following standard is mandated for DoD systems that are required to exchange security attributes, for example sensitivity labels:

- MIL-STD-2045-48501, Common Security Label, 25 January 1995.

6.2.3.3 Transmission Media Security Standards

There are currently no security standards mandated for transmission media.

6.2.4 Information Modeling And Information Security Standards

At this time, no information modeling and information security standards are mandated. It should be noted that process models and data models produced should be afforded the appropriate level of protection.

6.2.5 Human-Computer Interface (HCI) Security Standards

DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria (TCSEC), December 1985, specifies the minimal security requirements associated with a required level of protection for DoD automated systems. HCI security-related requirements may include authentication, screen classification display, and management of access control workstation resources.

For systems employing graphical user interfaces, the following guideline is mandated:

- DoD Human-Computer Interface Style Guide, TAFIM Version 2.0, Volume 8, 30 September 1994.

6.3 EMERGING STANDARDS

The standards listed in this subsection are expected to be elevated to mandatory status when implementations of the standards mature.

6.3.1 Introduction

The emerging security standards described in this section are drawn from work being pursued by ISO, IEEE, IETF, Federal standards bodies, and consortia such as the Object Management Group (OMG). Section 6.3 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related subject area in the sections of the JTA (information, processing, information transfer, information modeling and information exchange, and human-computer interface) and their subsections.

6.3.2 Information Processing Security Standards

Information processing security standards are emerging in the following areas: application software entity and application platform entity (software engineering, operating systems, and distributed computing services).

6.3.2.1 Application Software Entity Security Standards

Emerging application software entity standards include evaluation criteria and WWW security-related standards.

6.3.2.1.1 Evaluation Criteria Security Standards

The Common Criteria for Information Technology Security Evaluation (CC) is an effort by the governments of North American and European nations to develop a common criteria for developing trusted information technology products that can be used to help protect important information of government and private sectors. It uses input from the European Information Technology Security Evaluation Criteria (ITSEC), the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), the U.S. draft Federal Criteria for Information Technology Security, and the TCSEC (DoD 5200.28-STD). CC Version 1.0 is undergoing international review and testing for use in evaluations of products prior to being fully accepted within Europe and North America. The CC is expected to replace DoD 5200.28-STD. Common Criteria (Parts 1-3) has been formally adopted by ISO as the basis for its future work in security criteria. The reference to the ISO adopted CC is "ISO/IEC JTC1/SC27/WG3 N304, 23 April 1996".

6.3.2.1.2 World Wide Web Security Standards

"The Secure Sockets Layer (SSL) Protocol Version 3.0", A. Freier, P. Karlton, P. Kocher, 13 March 1996, draft-freier-ssl-version3-01.txt, an Internet Draft supporting WWW security, is being considered for standardization. The SSL protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. SSL runs above the transport layer.

6.3.2.2 Application Platform Entity Security Standards

For the application platform entity, security standards are emerging for software engineering, operating systems, and distributed computing services.

6.3.2.2.1 Software Engineering Services Security

For software engineering services, security standards are emerging for Generic Security Service (GSS)-Application Program Interface (API) and POSIX areas.

6.3.2.2.1.1 Generic Security Service (GSS)-Application Program Interface (API) Security

The GSS-API, as defined in RFC-1508, September 1993 (IETF), provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments. RFC-1508 defines GSS-API services and primitives at a level independent of underlying mechanism and programming language environment. The Internet Draft "GSS-API, Version 2," J. Linn, 20 February 1996, draft-ietf-cat-gssv2-05.txt revises RFC-1508, making specific, incremental changes in response to implementation experience and liaison requests.

The Internet Draft, "Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)," C. Adams, 18 February 1996, draft-ietf-cat-idup-gss-04.txt, extends the GSS-API (RFC-1508) for non-session protocols and applications requiring protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated "receivers" of the data unit. An example application is secure electronic mail where data needs to be protected without any on-line connection with the intended recipient(s) of that data. Subsequent to being protected, the data unit can be transferred to the recipient(s) - or to an archive - perhaps to be processed as unprotected only days or years later.

6.3.2.2.1.2 POSIX Security Standards

The following draft IEEE standards define a standard interface and environment for POSIX-based computer operating systems that require a secure environment: IEEE P1003.1e, POSIX Part 1: System API - Protection, Audit, and Control Interfaces [C Language], Draft 15 (reballot March 1996) and IEEE P1003.2c, POSIX Part 2: Shell and Utilities - Protection and Control Interfaces, Draft 15 (reballot March 1996). These draft standards define security interfaces to open systems for access control lists, audit, privilege, mandatory access control, and information label mechanisms and are stated in terms of their C bindings.

6.3.2.2.2 Operating System Services Security

Operating system services security standards are emerging in the following areas: evaluation criteria and authentication.

6.3.2.2.2.1 Evaluation Criteria Security Standards

See section 6.3.2.1.1 for description of the following emerging standard that is expected to replace DoD 5200.28-STD: Common Criteria for Information Technology Security Evaluation.

6.3.2.2.2.2 Authentication Security Standards

RFC-1938, A One-Time Password System, provides authentication for system access (login) and other applications requiring authentication that is secure against passive attacks based on replaying captured reusable passwords. The One-Time Password System evolved from the S/KEY One-Time Password System that was released by Bellcore.

6.3.2.2.3 Distributed Computing Services Security Standards

DCE Authentication and Security Specification (P315) is a draft Open-Group Specification for DCE.

The Common Object Request Broker Architecture (CORBA), OMG 95-12-1, December 1995, is emerging. CORBA Security Services define a software infrastructure that supports access control, authorization, authentication, auditing, delegation, non-repudiation, and security administration for distributed object-based systems. This infrastructure can be based on existing security environments and can be used with existing permission mechanisms and login facilities. The key security functionality is confined to a trusted core that enforces the essential security policy elements. Since the CORBA Security Services are intended to be flexible, two levels of conformance may be provided. Level 1 provides support for a default system security policy covering access control and auditing. Level 1 is intended to support applications that do not have default policy. Level 2 provides the capability for applications to control the security provided at object invocation and also for applications to control the administration of an application-specific security policy. Level 2 is intended to support multiple security policies and to provide the capability to select separate access control and audit policies.

6.3.3 Information Transfer Security Standards

Security standards are emerging for the following information transfer areas: end systems (host standards) and network (internetworking standards).

6.3.3.1 End System Security Standards

Emerging end system security standards include host standards discussed in the following subsection.

6.3.3.1.1 Host Security Standards

Security standards are emerging for host end systems in the security protocols and public key infrastructure areas discussed in the following subsections.

6.3.3.1.1.1 Security Protocols

The Common Internet Protocol (IP) Security Options (CIPSO) of the following emerging standard is expected to adopt MIL-STD-2045-48501, Common Security Label: Trusted Systems Interoperability Group (TSIG) Trusted Information Exchange for Restricted Environments (TSIX (RE)) 1.1.

The following Integrated Services Digital Network (ISDN) security protocol is emerging: ISP-421, Revision 1.0: The ISDN Security Program (ISP) Security Association Management Protocol (SAMP), 15 May 1994.
The following are emerging standards for Local Area Network (LAN) security: IEEE 802.10c/D13, Standard for Interoperable LAN Security-Part C: Key Management, and IEEE 802.10g/D7, Standard for Interoperable LAN Security - Part G: Standard for Security Labeling within Secure Data Exchange.

MIL-STD-2045-18500 is based on Version 3.0 of the MSP documented in SDN 701. MSP is under revision to Version 4.0 to accommodate, in part, Allied requirements. When the revision to MSP is completed DoD is expected to move to MSP Version 4.0.

6.3.3.1.1.2 Public Key Infrastructure Security Standards

The emerging FIPS PUB JJJ is based on ISO/IEC 9798-3: 1993, Entity Authentication Using a Public Key System and will provide a standard for Public Key Cryptographic Entity Authentication Mechanisms for use in public key based challenge-response and authentication systems at the application layer within computer and digital telecommunications systems.

6.3.3.2 Network Security Standards

Emerging network standards are listed in subsection 6.3.3.2.1.

6.3.3.2.1 Internetworking Security Standards

RFC-1825, "Security Architecture for the Internet Protocol," R. Atkinson, August 1995, describes the security mechanisms for IP version 4 (IPv4) and IP version 6 (IPv6) and the services that they provide. Each security mechanism is specified in a separate document. RFC-1825 also describes key management requirements for systems implementing those security mechanisms. It is not an overall Security Architecture for the Internet, but focuses on IP-layer security.

RFC-1826, "IP Authentication Header (AH)," R. Atkinson, August 1995, describes a mechanism for providing cryptographic authentication for IPv4 and IPv6 datagrams. An AH is normally inserted after an IP header and before the other information being authenticated. The AH is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed.

RFC-1827, "IP Encapsulating Security Payload (ESP)," R. Atkinson, August 1995, discusses a mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances, depending on the encryption algorithm and mode used, it can also provide authentication to IP datagrams. Otherwise, the IP AH may be used in conjunction with ESP to provide authentication. The mechanism works with both IPv4 and IPv6.

The Domain Name System (DNS) has become a critical operational part of the Internet infrastructure yet it has no strong security mechanisms to assure data integrity or authentication. DNS Security Extensions, D. Eastlake, C. Kaufman, 30 January 1996, draft ietf dnssec-secext-09.txt, describes extensions to the DNS that provide these services to security aware resolvers or applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. Security can still be provided even through non-security aware DNS servers in many cases. The extensions also provide for the storage of authenticated public keys in the DNS. This storage of keys can support general public key distribution service as well as DNS security.

Three IEEE LAN standards are emerging: IEEE 802.10, IEEE Standards for Local and Metropolitan Area Networks (MANs): Interoperable LAN/MAN Security (SILS), 1992, discusses services, protocols, data formats, interfaces to allow IEEE 802 products to interoperate. It discusses authentication, access control, data integrity, and confidentiality. IEEE 802.10a, Standard for Interoperable LAN Security-The Model, Draft Jan 1989 shows the relationship of SILS to OSI and describes required interfaces. IEEE 802.10b, Standard for Interoperable LAN Security-Part B: Secure Data Exchange, 1992 deals with secure data exchange at the data link layer.

6.3.4 Information Modeling and Information Security Standards

There are no emerging standards in this area at this time.

6.3.5 Human-Computer Interface (HCI) Security Standards

Refer to section 6.3.2.1.1 for information pertaining to the following emerging standard that is expected to replace DoD 5200.28-STD:. Common Criteria for Information Technology Security Evaluation.

Refer to section 6.3.3.1.1.2 for information pertaining to FIPS PUB JJJ, Standard for Public Key Cryptographic Entity Authentication Mechanisms.

JTA APPENDIX A - ACRONYMS

AAL	ATM Adaptation Layer
ABOR	Abort
ACP	Allied Communication Publication
ACTD	Advanced Concept Technology Demonstration
AES	Application Environment Specification
AH	Authentication Header
ALE	Automated Link Establishment
ALSP	Aggregate Level Simulation Protocol
ANSI	American National Standards Institute
API	Application Programming Interface
ARIDPCM	Adaptive Recursive Interpolated Differential Pulse Code Modulation
ARP	Address Resolution Protocol
ASD	Assistant Secretary of Defense
ATA	Army Technical Architecture
ATD	Advanced Technology Demonstration
ATIS	Alliance for Telecommunication Industry Solutions
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
BER	Bit Error Rate
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
bps	Bits Per Second
BRI	Basic Rate Interface
BUFR	Binary Universal Format for Representation
C/S/A	CINCs/Services/Agencies
C2	Command and Control
C2CDM	Command and Control Core Data Model
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CADRG	Compressed Arc Digitized Raster Graphics
CAE	Common Application Environment
CALS	Continuous Acquisition and Life Cycle Support
CASE	Computer Automated Software Engineering
CBS	Commission for Basic Systems
CC	Common Criteria for Information Technology Security Evaluation
CCB	Change Control Board
CCITT	International Telegraph & Telephone Consultative Committee (now ITU)
CDE	Common Desktop Environment
CDENext	Next Version of CDE
CDMA	Code Division Multiple Access
CFS	Center for Standards

CG	Commanding General
CGI	Computer Graphics Interface
CGM	Computer Graphics Metafile
CIB	Controlled Image Base
CIDE	Communication Information Data Exchange
CINC	Commander In Chief
CIO	Central Imagery Office
CIPSO	Common Internet Protocol Security Options
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Memo
CM	Configuration Management
CMMS	Conceptual Models of the Mission Space
CNR	Combat Net Radio
COE	Common Operating Environment
CONUS	Continental United States
CORBA	Common Object Request Broker Architecture
COSE	Common Open Software Environment
COTS	Commercial Off-the-Shelf
CRM	Computer Resources Management
CSMA/CD	Carrier Sense Multiple Access / Collision Detection
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria

DAA	Designated Approving Authority
DAMA	Demand Assigned Multiple Access
DBDB	Digital Bathymetric Database
DBMS	Database Management System
DCA	Defense Communications Agency (now DISA)
DCAC	Defense Communications Agency Circular (now DISA)
DCE	Distributed Computing Environment
DDDS	Defense Data Dictionary System
DDM	DoD Data Model
DDRS	Defense Data Repository System
DEF	Data Exchange Format
DGSA	DoD Goal Security Architecture
DHCP	Dynamic Host Configuration Protocol
DIA	Defense Intelligence Agency
DIGEST	Digital Geographic Information Exchange Standard
DII	Defense Information Infrastructure
DIS	Distributed Interactive Simulation
DIS	Draft International Standard
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DLWG	Data Link Working Group
DMA	Defense Mapping Agency
DMAL	Defense Mapping Agency List
DMS	Defense Message System
DMTD	Digital Message Transfer Device
DNC	Digital Nautical Chart
DNS	Domain Name System
DoD	Department of Defense
DoDD	DoD Directive

DoDISS	DoD Index of Specifications and Standards
DoDSSP	DoD Single Stock Point
DPPDB	Digital Point Positioning Data Base
DSIC	Defense Standards Improvement Council
DSN	Defense Switched Network
DSP	Defense Standardization Program
DTED	Digital Terrain Elevation Data
DTOP	Digital Topographic Data
EEI	External Environment Interface
EHF	Extremely High Frequency
EIA	Electronics Industries Association
E-MAIL	Electronic Mail
ESP	Encapsulating Security Payload
FAQ	Frequently Asked Questions
FDDI	Fiber Distributed Data Interface
FDMA	Frequency Division Multiple Access
FED-STD	Federal Telecommunication Standard
FIPS	Federal Information Processing Standards
FPLMTS	Future Public Land Mobile Telecommunications Systems
FTP	File Transfer Protocol
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIF	Graphics Interchange Format
GIS	Geographic Information System
GKS	Graphical Kernel System
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GRIB	Gridded Binary
GSS	Generic Security Service
GUI	Graphical User Interface
HCI	Human-Computer Interface
HF	High Frequency
HITL	Human-in-the-Loop
HLA	High Level Architecture
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I&RTS	Integrated and Runtime Specification
IAB	Internet Architecture Board
ICCCM	Inter-Client Communications Convention Manual
ICMP	Internet Control Message Protocol
IDEF	Integrated (Computer-Aided Manufacturing) Definition
IDEF1X	Integrated Definition for Information Modeling

IDEF0	Integrated Definition for Function Modeling
IDUP	Independent Data Unit Protection
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IER	Information Exchange Requirements
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IGMP	Internet Group Management Protocol
IMETS	Integrated Meteorological System
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPv4	IP Next Generation/Version 4
IPv6	IP Next Generation/Version 6
IS	Information System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	International Standardized Profile
ISP	ISDN Security Program
ISS	Intelligence Systems Secretariat
ITSEC	European Information Technology Security Evaluation Criteria
ITSG	Information Technology Standards Guidance
ITU	International Telecommunications Union (formerly called CCITT)
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector
JCSA	Joint C4ISR System Architecture
JFIF	JPEG File Interchange Format
JIEO	Joint Interoperability & Engineering Organization
JPEG	Joint Photographic Expert Group
JTA	Joint Technical Architecture
JTA WG	Joint Technical Architecture Working Group
JTDLMP	Joint Tactical Data Link Management Plan
JTIDS	Joint Tactical Information Distribution System
kbps	Kilobits Per Second
kHz	Kilohertz
KMP	Key Management Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LDR	Low Data Rate
LOS	Line-of-Sight
LWD	Littoral Warfare Data
M&S	Modeling and Simulation
MAGTF	Marine Air Ground Task Force
MAN	Metropolitan-Area Network

MAU	Medium-Access Unit
Mbits/s	Megabits per second
MC&G	Mapping, Charting and Geodesy
MCCDC	Marine Corps Combat Development Command
MDR	Medium Data Rate
MHP	Mobile Host Protocol
Mhz	Megahertz
MIB	Management Information Base
MIDB	Management Information Database
MIDS	Multi-functional Information Distribution System
MIL-HDBK	Military Handbook
MILSATCOM	Military Satellite Communications
MIL-STD	Military Standard
MISSI	Multilevel Information Systems Security Initiative
MOSPF	Multicast Open Shortest Path First
MPEG	Motion Pictures Expert Group
MSMP	Modeling and Simulation Master Plan
MSP	Message Security Protocol

NATO	North Atlantic Treaty Organization
NCSC	National Computer Security Center (see NSA)
NIST	National Institute of Standards and Technology
NITFS	National Imagery Transmission Format Standard
NSA	National Security Agency
NTIS	National Technical Information Service
NTP	Network Time Protocol

ODBC	Open Data Base Connectivity
ODMG	Object Data Management Group
OLE	Object Linking Embedding
OMA	Object Management Architecture
OMG	Object Management Group
OODBMS	Object-Oriented Database Management System
OOM	Object-Oriented Methods
OOT	Object Oriented Technology
OSD	Office of the Secretary of Defense
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PCAT	PC Access Tool
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Services
PDU	Protocol Data Units
PHIGS	Programmers Hierarchical Interactive Graphics Systems
PM	Program Manager
PN-NI	Private Network-Network Interface
POC	Point of Contact
POSIX	Portable Operating System for Information Exchange

PPP	Point-to-Point Protocol
PPS	Precise Position Service
PRI	Primary Rate Interface
PSK	Phase Shift Keying
PSM	Persistent Stored Modules
PST	Prestructured Technology
PSTN	Public Switched Telephone Networks
RDBMS	Relational Database Management System
RF	Radio Frequency
RFC	Request for Comments
RFP	Requests for Proposals
RPC	Remote Procedure Call
RPF	Raster Product Format
RTI	Run Time Infrastructure
SAMP	Security Association Management Protocol
SATCOM	Satellite Communications
SCC	Standards Coordinating Committee
SDN	Secure Data Network
SDNS	Secure Data Network System
SEDRIS	Synthetic Environment and Data Representation Interchange Specification
SGML	Standard Generalized Markup Language
SHF	Super High Frequency
SIDR	Secure Intelligence Data Repository
SILS	Standard for Interoperable LAN Security
SNMP	Simple Network Management Protocol
SNMPv1	Structure of Management Information
SONET	Synchronous Optical Network
SOW	Statements of Work
SSL	Secure Socket Layer
STANAG	Standardization Agreement
STD	Standard
STOU	Store Unique
STS	Synchronous Transport Signal
SUS	Single UNIX Specification
TACO2	Tactical Communications Protocol 2
TADIL	Tactical Digital Information Link
TAFIM	Technical Architecture Framework for Information Management
TAWDS	Tactical Automated Weather Distribution System
TCP	Transmission Control Protocol
TCSEC	Trusted Computer Security Evaluation Criteria
TDL	Tactical Data Link
TDMA	Time Division Multiple Access
TELNET	Telecommunications Network
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TIDP	Technical Interface Design Plan

TIS	Technical Interface Specification
TOS	Type-of-Service
TP0	Transport Protocol Class 0
TRC	Technical Reference Code
TRM	Technical Reference Model
TSIG	Trusted Systems Interoperability Group
TSIX(RE)	Trusted Security Information Exchange for Restricted Environments
UCS	Universal Multiple-Octet Coded Character Set
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UI	User Interface
UNI	User-Network Interface
URL	Uniform Resource Locator
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USIS	United States Imagery System
USMC	U.S. Marine Corps
USMTF	United States Message Text Format
UVMap	Urban Vector Map
VHF	Very High Frequency
VITD	Vector Product Interim Terrain Data
VMap	Vector Map
VMap AD	VMap Aeronautical Data
VMF	Variable Message Format
VPF	Vector Product Format
VTC	Video Teleconferencing
WGS	World Geodetic System
WMO	World Meteorological Organization
WNDP	Worldwide Numbering and Dialing Plan
WVS+	World Vector Shoreline Plus
WWW	World Wide Web

JTA APPENDIX B - LIST OF MANDATED STANDARDS AND SOURCES

This appendix summarizes the mandated standards from the Joint Technical Architecture (JTA), and provides references to locations where the standards may be obtained. The mandated standards from Sections 2 through 6 are summarized in a set of tables, with one table per section. The first column in each table contains a reference to the JTA section where the standards is mandated. When there are multiple standards mandated in a section, only the first standard contains a reference.

The second column contains the full citation for the mandated standard, including an identifying number, date, and title. Where the standards are available electronically, the tables contain an electronic link to the standard. These links are accessible in the on-line World Wide Web (WWW) version of the JTA.

If the mandated standard is based on other standards (e.g. it is a Government profile of one or more industry standards), the third column identifies the "base standards" that are referenced by the mandated standard. These are included a convenience to allow greater understanding of the scope of these mandated standards. Depending on how the base standards are referenced in the mandated standard, part or all of the base standards may implicitly also be mandated.

The second part of this appendix provides instructions for obtaining copies of the standards cited in the JTA. Where possible, this section also contains electronic links to the appropriate organization, accessible in the WWW version of the JTA.

Information Processing Mandated Standards

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
2.2.2.1.2 User Interface Services	FIPS Pub 158-1: 1993, User Interface Component of the Application Portability Profile, X-Windows Version 11, Release 5	
	OSF Motif Application Environment Specification (AES) Release 1.2, 1992	
	OSF/Motif Motif Inter Client Communications Convention Manual (ICCCM)	
	Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993, Microsoft Press	
	X/Open C323 Common Desktop Environment (CDE) Version 1.0, April 1995	
2.2.2.1.3 Data Management Services	FIPS Pub 127-2: 1993, Database Language for Relational DBMS	ISO 9075: 1992 Database Language for Relational DBMSs
	Open Database Connectivity ODBC 2.0	
2.2.2.1.4.1 Document Interchange	ISO 8879: 1986, Standard Generalized Markup Language (SGML)	
	RFC-1866: 1995, Hypertext Markup Language (HTML), Internet Version 2.0	
2.2.2.1.4.2 Graphics Data Interchange	FIPS Pub 128-1: 1993, Computer Graphics Metafile (CGM) - Interchange format for vector graphics data	ISO 8632.1-4: 1992 Computer Graphics Metafile (CGM) - Interchange format for vector graphics data.
	JPEG File Interchange Format (JFIF), Version 1.02, C-Cube Microsystems for raster graphics data	ISO/IEC 10918-1: 1994 Joint Picture Expert Group (JPEG) algorithm
2.2.2.1.4.3 Geospatial Data Interchange	MIL-STD-2411, Raster Product Format (RPF)	
	MIL-STD-2407, Interface Standard for Vector Product Format (VPF)	
	MIL-STD-2401, World Geodetic System 84 (WGS-84), 21 March 1994	
	DMAL 805-1A, DMA List of Products and Services, March 1994	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
2.2.2.1.4.4 Imagery Data Interchange	MIL-STD-2500A, National Imagery Transmission Format (Version 2.0) for file format	
	MIL-STD-188-196, Bi-Level Image Compression	
	MIL-STD-188-199, Vector Quantization Decompression	
	MIL-STD-2301	ANSI/ISO 8632:1992 Computer Graphics Metafile (CGM)
	ISO/IEC 10918-1: 1994, Joint Photographic Experts Group (JPEG), as profiled by MIL-STD-188-198A	
2.2.2.1.4.6 Sound Data Interchange	ISO/IEC 11172-1:1993 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems	
	ISO/IEC 11172-3:1993 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 3: Audio	
	ISO/IEC 11172-3/Cor. 1:1995 - Encoding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 3: Audio Technical Corrigendum	
	ISO DIS 13818-1: 1996, Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems	
	ISO DIS 13818-3: 1995, Generic Coding of Moving Pictures and Associated Audio Information - Part 3: Audio	
2.2.2.1.4.7 Video Data Interchange	ISO/IEC 11172-1: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems	
	ISO/IEC 11172-1: 1993/Cor. 1:1995 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 1: Systems Technical Corrigendum 1	
	ISO/IEC 11172-2: 1993 Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbits/s -- Part 2 Video	
	ISO DIS 13818-1: 1996, Generic Coding of Moving Pictures and Associated Audio Information - Part 1: Systems	
	ISO DIS 13818-2: 1996 - Generic Coding of Moving Pictures and Associated Audio Information - Part 2: Video	
2.2.2.1.4.8 Atmospheric Data Interchange	FM 92-X-GRIB, The WMO Format for the Storage of Weather Product Information and the Exchange of Weather Product Messages in Gridded Binary (GRIB) Form	
	FM 94-X-BUFR, The WMO Binary Universal Format for Representation (BUFR) of meteorological data.	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
	Data Exchange Format (DEF), Appendix 30 to the TAWDS/IMETS Implementation Document for Communication Information Data Exchange (CIDE)	
2.2.2.1.4.9 Oceanographic Data Interchange	FM 94-X-BUFR, The WMO Binary Universal Format for Representation (BUFR) of oceanographic data.	
2.2.2.1.5 Graphic Services	ISO 7942: 1985, as profiled by FIPS Pub 120-1 (change notice 1): 1991, Graphical Kernel System (GKS) - for 2-D graphics	
	ISO 9592: 1989, as profiled by FIPS Pub 153, Programmers Hierarchical Interactive Graphics Systems (PHIGS) - for 3-D graphics	
	ISO/IEC 9636: 1991, Information Technology-Computer Graphics-Interfacing (CGI) Techniques for Dialogue with Graphics Devices	
2.2.2.1.7 Operating System Services	ISO 9945-1: 1990, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 1: System Application Program Interface (API) [C language], (as profiled by FIPS PUB 151-2: 1993)	
	ISO 9945-2: 1993, Information Technology - Portable Operating System Interface for Computer Environments (POSIX) - Part 2: Shell and Utilities, (as profiled by FIPS PUB 189: 1994)	
	IEEE 1003.2d: 1994, POSIX - Part 2: Shell and Utilities - Amendment: Batch Environment	
	IEEE 1003.1b: 1993, POSIX - Part 1: System Application Program Interface (API) Amendment 1; Real Time Extension [C Language]*, (as profiled by FIPS Pub 151-2: 1993)	
	IEEE 1003.1i: 1995, POSIX - Part 1: System Application Program Interface (API) Amendment: Technical Corrigenda to Real-time Extension [C Language]*	
	IEEE 1003.1c: 1995 POSIX - Part 1: System Application Program Interface (API) Amendment 2: Threads Extension [C Language]	
	Win32 APIs, Window Management and Graphics Device Interface, Volume 1 Microsoft Win32 Programmers Reference Manual, 1993, Microsoft Press.	
2.2.2.2.1 Internationalization Services	ISO/IEC 8859-1:1987, Information Processing - 8-Bit Single-Byte Coded Character Sets - Part 1: Latin Alphabet No. 1	
	ISO/IEC 10646-1:1993, Information Technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane	
2.2.2.2.4.1 Remote Procedure Computing	OSF -DCE Remote Procedure Call (RPC), Version 1.1, 1994	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
	OSF - DCE Time Services, Version 1.1, 1994	
	OSF - DCE Directory Services, Version 1.1, 1994	
2.2.2.2.4.2 Distributed Object Computing	OMG - The Common Object Request Broker: Architecture and Specification (CORBA), Version 2: July 1995, (also available as: X/Open Common Application Environment (CAE) Specification P431 - Common Object Request Broker Architecture & Specification, Version 2)	
	OMG - CORBA services: Common Object Services Specification, March 1996 (also available as: X/Open CAE Specification P432 - Common Object Services, Volume 1 and X/Open CAE Specification P502 - Common Object Services, Volume 2)	
	OMG - CORBA facilities: Common Object Facilities Architecture, November 1995	

Information Transfer Mandated Standards

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
3.2.1.1 Host Standards	IAB-Standard-3/RFC-1122/RFC-1123, Host Requirements, October 1989	
3.2.1.1.1.1 Electronic Mail	ACP 123 US Supplement No 1, Common Messaging Strategy and Procedures, November 1995	ACP 123:194 ISO/IEC 8613-1:1993 ISO/IEC 8859:1990 ISO/IEC 10021-1:1990 ISO/IEC 10021-2:1990 ISO/IEC 10021-4:1990 ISO/IEC 10021-5:1990 ISO/IEC 10021-6:1990 ISO/IEC 10021-7:1990 ISO/IEC ISP 10610-1: 1993 ISO/IEC ISP 10611-1: 1994 ISO/IEC ISP 10611-3: 1994 ISO/IEC ISP 10611-4: 1994 ISO/IEC ISP 10611-5: 1994 ISO/IEC ISP 12062-1: 1994 ISO/IEC ISP 12062-2: 1994 ITU X.400:1992 ITU X.402:1992 ITU X.411:1992 ITU X.413:1992 ITU X.419:1992 ITU X.420:1992 AMH2n (D) AMH9n (D) (MIL-STD-2045-18500)
3.2.1.1.1.2.1 X.500 Directory Services	ITU-T X.500, The Directory -- Overview of Concepts, Models and Services - Data Communication Networks Directory, 1993	
3.2.1.1.1.2.2 Domain Name System (DNS)	IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987	
3.2.1.1.1.3 File Transfer	IAB Standard 9/RFC-959, File Transfer Protocol, October 1985	
3.2.1.1.1.4 Remote Terminal	IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
3.2.1.1.1.5 Network Management	IAB Standard 15/RFC-1157, Simple Network Management Protocol (SNMP), May 1990	
	IAB Standard 16/RFC-1155/RFC-1212, Structure of Management Information , May 1990	
	IAB Standard 17/RFC-1213, Management Information Base, March 1991	
3.2.1.1.1.6 Network Time	RFC-1305, Network Time Protocol (V3), April 9, 1992	
3.2.1.1.1.7 Bootstrap Protocol (BOOTP)	RFC- 951, Bootstrap Protocol, September 1, 1985	
	RFC-1533, DHCP Options and BOOTP Vendor Extensions, October 8, 1993	
	RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993	
3.2.1.1.1.8 Dynamic Host Configuration Protocol (DHCP)	RFC-1541, Dynamic Host Configuration Protocol, October 27, 1993	
3.2.1.1.1.9.1 Hypertext Transfer Protocol (HTTP)	RFC-1945, Hypertext Transfer Protocol -- HTTP/1.0, May 17, 1996	
3.2.1.1.1.9.2 Uniform Resource Locator (URL)	RFC-1738, Uniform Resource Locators, December 20, 1994	
	RFC-1808, Relative Uniform Resource Locators, June 14, 1995	
3.2.1.1.1.10 Connectionless Data Transfer	MIL-STD-2045-47001, Connectionless Data Transfer Application Layer Standard, July 27, 1995	
3.2.1.1.2.1.1 Transmission Control Protocol (TCP)	IAB-Standard 7/RFC-793, Transmission Control Protocol, September 1981	
3.2.1.1.2.1.2 User Datagram Protocol (UDP)	IAB-Standard 6/RFC-768, User Datagram Protocol, August 1980	
3.2.1.1.2.1.3 Internet Protocol (IP)	IAB-Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/ RFC-792/RFC-1112, Internet Protocol, September 1981	
3.2.1.1.2.2 OSI/Internet Interworking Protocol	IAB-Standard 35/RFC-1006, ISO Transport Service on top of the TCP, May 1987	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
3.2.1.2 Video Teleconferencing (VTC) Standards	VTC001, Industry Profile for Video Teleconferencing, Revision 1, April 25, 1995	
	ITU-T H.324, Terminal for Low Bit Rate Multimedia Communications, March 19, 1996	
3.2.1.3.1 Analog Facsimile Standards	TIA/EIA-465-A, Group 3 Facsimile Apparatus for Document Transmission, March 21, 1995	
	TIA/EIA-466, Procedures for Document Facsimile Transmission, May 1981	
3.2.1.3.2 Digital Facsimile Standard	MIL-STD 188-161D, Interoperability and Performance Standards for Digital Facsimile Equipment, January 10, 1995	
3.2.1.4 Secondary Imagery Dissemination Standards	MIL-STD-2045-44500, National Imagery Transmission Standard (NITFS) Tactical Communications Protocol 2 (TACO2), June 18, 1993	
3.2.2.1 Router Standards	RFC-1812, Requirements for IP Version 4 Routers, June 22, 1995	
	IAB Standard 6/RFC-768, User Datagram Protocol, August 1980	
	IAB Standard 7/RFC-793, Transmission Control Protocol, September 1981	
	IAB Standard 8/RFC-854/RFC-855, TELNET Protocol, May 1983	
	IAB Standard 13/RFC-1034/RFC-1035, Domain Name System, November 1987	
	IAB Standard 15/RFC-1157, Simple Network Management Protocol, May 1990	
	IAB Standard 16/RFC-1155/RFC-1212, Structure of Management Information, May 1990	
	IAB Standard 17/RFC-1213, Management Information Base, March 1991	
	RFC-951, Bootstrap Protocol, September 1, 1985	
	RFC-1533, DHCP Options and BOOTP Vendor Extensions, October 8, 1993	
	RFC-1541, DHCP, October 27, 1993	
	RFC-1542, Clarifications and Extensions for the Bootstrap Protocol, October 27, 1993	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
	IAB Standard 33/RFC-1350, Trivial FTP (TFTP), July 1992, to be used for initialization only.	
3.2.2.1.1 Internet Protocol (IP)	IAB Standard 5/RFC-791/RFC-950/RFC-919/RFC-922/ RFC-792/RFC-1112, Internet Protocol, September 1981	
3.2.2.1.2.1 Interior Routers	RFC-1583, Open Shortest Path First Routing Version 2, for unicast routing, March 23, 1994	
	RFC-1584, Multicast Extensions to OSPF, March 24, 1994, for multicast routing	
3.2.2.1.2.2 Exterior Routers	RFC-1771, Border Gateway Protocol 4, March 21, 1995	
	RFC-1772, Application of BGP In the Internet, March 21, 1995	
3.2.2.2.1 Local Area Network (LAN)	ISO/IEC 8802-3: 1993, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, 10BaseT Medium-Access Unit (MAU)	
	IAB Standard 41/RFC-894, Standard for the Transmission of IP Datagrams Over Ethernet Networks, April 1984	
	IAB Standard 37/RFC-826, An Ethernet Address Resolution Protocol, November 1982	
3.2.2.2.2 Point to Point Standards	IAB Standard 51/RFC-1661/RFC-1662, Point-to-Point Protocol (PPP), July 1994	
	RFC-1332, PPP Internet Protocol Control Protocol (IPCP), May 26, 1992	
	RFC-1333, PPP Link Quality Monitoring, May 26, 1992	
	RFC-1334, PPP Authentication Protocols, October 20, 1992	
	RFC-1570, PPP Link Control Protocol (LCP) Extensions, January 11, 1994	
	EIA 232E, Interface Between Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, July 1991	
	EIA 449, General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit Terminating Equipment Employing Serial Binary Data Interchange, February 1980	
	EIA 530A, High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, June 1992, Including Alternate 26-Position Connector, 1992	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
3.2.2.2.3 Combat Net Radio (CNR) Networking	MIL-STD-188-220A, Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, July 27, 1995	
3.2.2.2.4 Integrated Services Data Network (ISDN)	ANSI T1.601, Telecommunications - Integrated Services Digital Network (ISDN) - Basic Access Interface for Use on Metallic loops for Application on the Network Side of the NT (Layer 1 Specification), 1992	
	ANSI T1.408, Telecommunications - Integrated Services Digital Network (ISDN) - Primary Rate - Customer Installation Metallic Interfaces (Layer 1 Specification), 1990	
	ITU-T Q.921, ISDN User-Network Interface - Data Link Layer Specification - Digital Subscriber Signaling System No. 1, 1993	
	ITU-T Q.931, ISDN User-Network Interface Layer 3 Specification for basic Call Control - Digital Subscriber Signaling System No. 1(DSS 1), Network Layer, User-Network Management, 1989	
	ITU-T E.164, Numbering Plan for the ISDN Era, 1991	
	DCAC 370-175-13, Defense Switched Network System Interface Criteria, section titled Worldwide Numbering and Dialing Plan (WNDP), September 1993	
	RFC-1356, Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode, August 6, 1992	
	RFC-1618, PPP over ISDN, May 13, 1994	
3.2.2.2.5 Asynchronous Transfer Mode (ATM)	ATM Forum's UNI Specification V 3.1, User-Network Interface, September 1994	
	ANSI T1.630 ATM Adaptation Layer for Constant Bit Rate Services Functionality and Specifications, 1993	
	ANSI T1.635 ATM Adaptation Layer Type 5 Common Part Functions and Specifications, 1994, which adopts ITU-T I.363, section 6	
	RFC-1577, Classical IP and Address Resolution Protocol (ARP) over ATM, January 20, 1994	
3.2.3.1.1.1 5- and 25-kHz Service	MIL-STD-188-181, Interoperability Standard for Dedicated 5-kHz and 25-kHz UHF Satellite Communications, September 18, 1992	
3.2.3.1.1.2 5-kHz DAMA Service	MIL-STD-188-182, Interoperability Standard for 5 kHz UHF DAMA Terminal Waveform, September 18, 1992	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
3.2.3.1.1.3 25-kHz TDMA/DAMA Service	MIL-STD-188-183, Interoperability Standard for 25 kHz UHF/TDMA/DAMA Terminal Waveform, September 18, 1992	
3.2.3.1.1.4 Data Control Waveform	MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, August 20, 1993	
3.2.3.1.2.1 Earth Terminals	MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, January 13, 1995	
3.2.3.1.2.2 Phase Shift Keying (PSK) Modems	MIL-STD-188-165, SHF Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), January 13, 1995	
3.2.3.1.3.1 Low Data Rate (LDR)	MIL-STD-1582, EHF LDR Uplinks and Downlinks, December 10, 1992	
3.2.3.1.3.2 Medium Data Rate (MDR)	MIL-STD-188-136, EHF MDR Uplinks and Downlinks, August 26, 1995	
3.2.3.2.1.1 Automated Link Establishment	MIL-STD-188-141A, Medium and High Frequency Radio Equipment Standard, September 10, 1993	
3.2.3.2.1.2 Anti-Jamming Capability	MIL-STD-188-148, Interoperability Standard Anti-Jam Communications (2-30 Mhz), April 13, 1992	
3.2.3.2.1.3 Data Modems	MIL-STD-188-110A, Data Modems, Interoperability and Performance Standards, September 30, 1991	
3.2.3.2.1.4 Very High Frequency (VHF)	MIL-STD-188-242, Tactical Single Channel (VHF) Radio Equipment, June 20, 1985	
3.2.3.2.1.5 Ultra High Frequency (UHF)	MIL-STD-188-243, Tactical Single Channel (UHF) Radio Communications, March 15, 1989	
3.2.3.2.1.6 Super High Frequency (SHF)	MIL-STD-188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, July 28, 1992	
3.2.3.2.5 JTIDS/MIDS Transmission Media	JTIDS System Segment Specification (Class 2 Terminal)	
	STANAG 4175, Edition 1, August 29, 1991 - Technical Characteristics of the Multifunctional Information Distribution System (MIDS)	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
3.2.3.3 SONET Transmissions	ANSI T1.105, Telecommunications - Synchronous Optical Network (SONET) - Basic Description Including Multiplex Structure, Rates and Formats (ATIS) (Revision and Consolidation of ANSI T1.105-1991 and ANSI T1.105A-1991), 1995	
	ANSI T1.107, Digital Hierarchy - Formats Specifications, 1995	
	ANSI T1.117, Digital Hierarchy - Optical Interface Specifications (SONET) (Single Mode - Short Reach), 1991	

Information Modeling and Information Mandated Standards

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
4.2.1 Activity model	FIPS PUB 183, Integration Definition for Function Modeling (IDEF0)	
4.2.2 Data Model	DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, January 1993	
	FIPS 184 Integration Definition for Information Modeling (IDEF1X)	
4.2.3 DoD Data Definitions	DoD Manual 8320.1-M-1, DoD Data Standardization Procedures, January 1993	
	Defense Data Dictionary System (DDDS), Version 3.2, May 1996	
4.2.4.2.1 J-Series Family of Message Standards	JTIDS Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 3 August 1994	
	STANAG 5516, Edition 1, Tactical Data Exchange - LINK 16, Ratified 2 March 1990	
	VMF Technical Interface Design Plan - Test Edition (TIDP-TE), Reissue 1 February 1995	
4.2.4.2.2 US Message Text Format (USMTF) Messages	MIL-STD-6040, United States Message Text Format (USMTF)	
4.2.4.2.3. Database-to-Database Exchange	Database-to-Database Exchange shall use standard data elements from DDDS, Version 3.2, May 1996	

Human-Computer Interfaces Mandated Standards

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
5.2.1 General	DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September, 1994.	
5.2.2.1 Commercial Style Guides	Open Software Foundation (OSF)/Motif™ Style Guide, Revision 1.2 (OSF 1992)	
	The Windows™ Interface: An Application Design Guide, Microsoft Press, 1992	
5.2.2.2 DoD HCI Style Guide	DoD HCI Style Guide, TAFIM Version 2.0, Volume 8, 30 September, 1994.	
5.2.2.3 Domain-level Style Guides	User Interface Specification for the Global Command and Control System (GCCS), October 1994	

Information Systems Security Mandated Standards

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
6.2.2.1 Application Software Entity Security Standards	DoD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria, December 1985	
	NCSC-TG-021, Version 1, Trusted Database Management System Interpretation, April 1991	
	FORTEZZA Application Implementors' Guide, MD4002101-1.52, 5 March 1996	
	FORTEZZA Cryptologic Programmers' Guide, MD4000501-1.52, 30 January 1996	
6.2.2.2.1 Operating System Services Security	DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985	
6.2.2.2.1.1 Security Auditing and Alarms Standards	ISO/IEC 10164-8, 1993, Information Technology-Open System Interconnection - Systems Management - Part 8: Security Audit Trail Function (ITU-T X.740)	
	DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985	
	ISO/IEC 10164-7, 1992, Information Technology-Open System Interconnection - Systems Management - Part 7: Security Alarm Reporting Function (ITU-T X.736, 1992)	
6.2.2.2.1.2 Authentication Security Standards	FIPS PUB 112, Password Usage, NIST, 30 May 1985	
	RFC-1510, The Kerberos Network Authentication Service, V.5, 10 September 1993	
6.2.3.1.1 Host Security Standards	FORTEZZA Interface Control Document, Revision P1.5, 22 December 1994	
	FORTEZZA Plus Interface Control Document, Release 3.0, 1 June 1995	
6.2.3.1.1.1 Security Algorithms	FIBS PUB 180-1, Secure Hash Standard, NIST, April 1995	
	FIPS PUB 186, Digital Signature Standard, NIST, May 1994	
	FIPS PUB 185, Escrowed Encryption Standard, NIST, 9 February 1994	
	Key Exchange Algorithm, NSA, R21-TECH-23-94, 12 July 1994	
6.2.3.1.1.2 Security Protocols	MIL-STD-2045-48501, Common Security Label	

JTA SECTION & SERVICE AREA	MANDATED STANDARD, TITLE, & DATE	BASE STANDARDS PROFILED
	ITU-T Rec. X.509 (ISO/IEC 9594-8.2), Version 3, The Directory: Authentication Framework (1993)	
	MIL-STD-2045-18500, Message Handling System Message Security Protocol (MSP) Profile, October 1993	NSA Documents SDN 701, 702, 703, 801, 802
	SDN.903, revision 3.2, Secure Data Network System (SDNS) Key Management Protocol (KMP), 1 August 1989	
6.2.3.1.1.3 Evaluation Criteria Security Standards	DoD 5200.28-STD, The DoD Trusted Computer System Evaluation Criteria, December 1985	
	NCSC-TG-005, Version-1, Trusted Network Interpretation, July 1987	
6.2.3.2.1 Internetworking Security Standards	FIPS PUB 185, Escrowed Encryption Standard, NIST, 9 February 1994	
	SDN.301, revision 1.5, Secure Data Network System (SDNS) Security Protocol 3 (SP3), 1989	
	MIL-STD-2045-48501, Common Security Label	
6.2.5 Human-Computer Interface (HCI) Security Standards	DoD Human-Computer Interface Style Guide, TAFIM, Version .2.0, Volume 8, 30 September 1994	

DOCUMENT SOURCES

Commercial Documents

- Copies of American National Standards Institute (ANSI) standards may be obtained from: American National Standards Institute, Attention Customer Service, 11 West 42nd St., New York, NY 10036 or call (212) 642-4900.
- Copies of International Telegraph and Telephone Consultative Committee (CCITT) standards may be obtained from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161 or call (703) 487-4650. [Note: The CCITT has changed its name to the International Telecommunications Union - Telecommunications Standardization Sector (ITU-T).]
- Copies of ISO standards may be obtained from: American National Standards Institute, Attention Customer Service, 11 West 42nd St., New York, NY 10036 or call (212) 642-4900.
- Copies of IEEE standards may be obtained from: Secretary, IEEE Standards Board, Institute of Electrical and Electronics Engineers, Inc., P.O. Box 1331, 445 Hoes Lane, Piscataway, NJ 08855-1331, USA or call 1 800 678-4333.
- A number of the standards mandated in this section are published by the Internet Architecture Board (IAB). The IAB is responsible for the Internet Protocol (IP) suite, and documents these protocols using Request for Comments (RFCs) and Standards (STDs). STDs are a subseries of notes within the RFC series that are formal Internet "Standards." The Internet Engineering Steering Group (IESG) has established certain RFCs as the official standard protocols for the Internet. All IAB documents are available free of charge via anonymous ftp in the directories under the URL: ftp://ds.internic.net/. RFCs are available, free of charge, via e-mail using the following address: mailserv@ds.internic.net. "Send rfcxxxx.txt" in the body. RFCs may also be obtained from: SRI International, Room EJ291, Network Information Systems Center, 333 Ravenswood Avenue, Menlo Park, CA 94025, USA.
- Copies of EIA standards may be obtained from Global Engineering Documents, 1 800 854-7179.
- World Meteorological Organization (WMO) documents may be obtained from the American Meteorological Society, Attention: WMO Publications Center, 45 Beacon Street, Boston, MA 02108.
- Open Group documents (was OSF and X/Open) may be obtained at Open Group, Apex Plaza, Foxbury Road, Reading, England, Fax# +44 734500110, or phone# +44 734508311.

Government Documents

- Copies of federal and military specifications, standards, and handbooks are available from: DoD Single Stock Point (DoDSSP) - Customer Service, Standardization Document Order Desk, 700 Robbins Avenue, Bldg. 4D, Philadelphia, PA 19111-5094. The DoDSSP has a Special Assistance Desk, Monday through Friday 7:30 A.M. - 4:00 P.M. (215) 697-2667/2179.
- Federal Information Processing Standards (FIPS) are available to DoD activities from: DoDSSP - Customer Service, as noted above. Others must request copies of FIPS from: National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161-2171.
- STANAG's and other NATO standardization agreements, in draft or ratified form, may be obtained by DoD, Federal agencies, and their contractors from the Central U.S. Registry, Pentagon. The specific short title, E.G., AC/301(PIII), subject, or STANAG number is needed to identify the document. Facility and personnel clearance verifications will be required to obtain classified NATO documents. Contractor requests for documents should be forwarded through their COR (contracting officer representative) or other Government sponsor to establish need-to-know. Contractors entering bid proposals and not yet having established a COR or government representative will be required to

provide a statement of work or the Contract Security Classification Specification (DD Form 254) of their classified contract. Requests to the Central U.S. Registry may be submitted in writing (3072 Army Pentagon, Washington, D.C. 20301-3072), by phone or by facsimile message: Telephone (703) 697-5943/6432, FAX (703) 693-0585.

- NIST documents can be obtained from: National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161-2171 or by calling (703) 487-4650.
- The Rainbow Series of Computer Security Documents may be obtained from NSA-V21, Address: 9800 Savage Rd., Fort Meade, MD 20755 or by calling (410) 859.6091.
- Multilevel Information Systems Security Initiative (MISSI) product information (FORTEZZA, etc.) may be obtained by calling the MISSI Help Desk on 1 800-GO-MISSI.
- The Technical Architecture Framework for Information Management (TAFIM) may be obtained by E-mail: tafim@bah.com or by calling the TAFIM Support Line on (703) 824-3743.
- The Information Technology Standards Guidance (ITSG) may be obtained from the Center for Standards (CFS) World Wide Web (WWW) page at http:\\www.itsi.disa.mil.
- VTC001 - Industry Profile for Video Teleconferencing may be obtained from the Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO) code JEBBC, Fort Monmouth, NJ 07703 or by calling (908) 532-7715.
- DISA and Defense Communications Agency (DCA) Circulars such as DCAC-370-175-13 may be obtained from the DISA Publications Office at FAX (703) 607-4661 with request written on company letterhead and noting contract number, or call (703) 607-6548.
- The Defense Data Dictionary System (DDDS) comes in two mediums, on-line and through a PC Access Tool (PCAT). DISA maintains both DDDS mediums. Developers should use both versions for full DDDS coverage. The PCAT comes in either diskette or CD-ROM and is published quarterly. Use PCAT first, then verify your findings with the continually updated DDDS on-line. Information about the DDDS is available from DISA JIEO, Center for Standards, 701 S. Courthouse Road, Arlington, VA 22204.
- Technical Interface Design Plans (TIDPs) may be obtained via the service POC's to the Joint Multi-TADIL CCB from the DISA/JIEO Center for Standards (CFS) TADIL Division, code JEBCA, chuaj@ncr.disa.mil or (703) 735-3524 or DSN 653-3524.
- Additional information concerning imagery related standards that apply to the United States Imagery System (USIS) can be found in CIO-2008, Version 1, 13 October 1995, USIS Standards & Guidelines.

JTA APPENDIX C - JTA RELATIONSHIP TO DOD STANDARDS REFORM

C.1 DOD (SPECIFICATIONS AND) STANDARDS REFORM - BACKGROUND

The DoD Standards Reform was begun in June 1994 when the Secretary of Defense issued his memorandum entitled "Specifications and Standards - A New Way of Doing Business." Secretary Perry directed that performance-based specifications and standards or nationally-recognized private sector standards be used in future acquisitions. He intends by this initiative to eliminate non-value added requirements, and thus to reduce the cost of weapon systems and materiel; remove impediments to getting commercial state-of-the-art technology into our weapon systems; and integrate the commercial and military industrial bases to the greatest extent possible. The Defense Standards Improvement Council (DSIC) directs implementation of the Reform. The DSIC has interpreted and extended the Reform policy through a series of numbered OSD policy memos. These policy memos and other DSIC decisions, newsletters and other standardization related information are posted on the Defense Standardization Program (DSP) Home Page at http://www.acq.osd.mil/es/std/.

C.2 THE JTA AND THE DOD STANDARDS REFORM

The standards and specifications and other standardization documents identified in the Joint Technical Architecture (JTA) can be cited in solicitations without conflicting with the DoD Standards Reform. All JTA documents have been granted Department-wide exemption from the waiver requirement by the Defense Standards Improvement Council. Mandatory application of JTA standardization documents to acquisition solicitations is authorized. Contrary to interpretations that have been made in the recent past by some DoD organizations, the DoD Standards Reform is not eliminating military standards and specifications nor precluding their use. What the Reform is trying to eliminate is the automatic development and imposition of military unique standards and specifications as the cultural norm. The JTA calls out non-Government standards in every case where it makes sense and where it will lead to the use of commercial products and practices that meet the DoD's needs. The JTA only calls out Military and Federal standards and specifications in those instances where no non-Government standard exists that is cost effective and meets the requirement or where the use of the non-Government standard must be clarified to enable interoperability of DoD systems.

C.3 REFORM WAIVER POLICY

Policy Memo 95-1 establishes procedures for waivers for use of specifications and standards cited as requirements in solicitations. These waiver procedures apply to the types of documents that fall under the province of the Defense Standardization Program and are indexed in the DoD Index of Standards and Specifications (DoDISS). Specifically of relevance to the JTA, Policy Memo 95-1 states that non-Government standards, Interface Standards, Federal Information Processing Standards (FIPS), and Performance Specifications do not require waivers. Also, Policy Memo 95-9 provides that international standardization agreements such as NATO STANAGs (and ACPs) do not require waivers. Federal Telecommunications Standards (FED-STDs) do not require a waiver when they qualify as interface standards. All of the above waiver-free document types encompass most of the documents cited in the JTA. The DSP Home Page provides lists of waiver-free documents and in the near future the DoDISS will indicate those documents that can be used without a waiver.

USMC SUPPLEMENT

USMC 1.1 INTRODUCTION

USMC 1.1.1 Purpose

This supplement to the Joint Technical Architecture (JTA) provides standards mandatory for use in the Marine Corps for service areas that do not appear in the JTA.

USMC 2.1 MANDATES

USMC 2.1.1 Introduction

This sections contains the mandatory standards and standard products for use within the Marine Corps. Where products are specified, their inclusion is the result of one or more competitive procurements scoped to include the entire Marine Corps.

USMC 2.1.2 Information Processing Standards

USMC 2.1.2.1 Minimum Desktop Computer Configuration and Software Product Requirements

This section adopts the DoD minimum desktop configuration for computers for the Marine Corps and adds certain requirements to support Marine Corps systems and infrastructure. Many new systems being planned for implementation within DoD, such as the Defense Message System (DMS), will provide only part of a whole system. The following minimum configurations satisfies those minimum capabilities which must exist on users' desktops if the users are to effectively meet their DoD missions on the existing and planned USMC infrastructure. The requirements of this section apply to all acquisitions of desktop computers.

The minimum desktop configuration for desktop automation terminals is designed to support user requirements such as connectivity to and operation within the Defense Information Infrastructure (DII), Global Command and Control System (GCCS), and DMS while also supporting local office automation applications. Table USMC-1 shows the desktop configuration for each of these systems and is provided as background. Support for new technology such as multimedia and various interface media such as Personal Computer Memory Card International Association (PCMCIA) slots used to support security in the DMS are included. Table USMC-2 shows the minimum desktop and server configurations for U.S. Marine Corps acquisitions and is mandated for acquisitions.

CG, MCCDC will publish a message each September which will specify the minimum Desktop Computer Configuration which may be purchased for the following Fiscal Year. This guidance will be based on requirements to support current missions as well as assumptions concerning future requirements. In compliance with Executive Order 12845, the above minimum desktop configuration must meet Environmental Protection Agency (EPA) Energy Star requirements.

Table USMC-1 - DoD Desktop System Configurations

DOD DESKTOP SYSTEM CONFIGURATIONS		
DMS	***GCCS***	***DII***
≥ 33 MHz clock speed ≥ 32-bit data path ≥ 8K of internal cache ≤ 5 volts ≥ 36 integer SPECmark ≥ 16 floating point SPECmark	≥ 66 MHz clock speed ≥ 32-bit data path ≥ 8K of internal cache ≤ 5 volts ≥ 36 integer SPECmark ≥ 16 floating point SPECmark	≥ 66 MHz clock speed ≥ 32-bit data path ≥ 8K of internal cache ≤ 5 volts ≥ 36 integer SPECmark ≥ 16 floating point SPECmark
16M RAM expandable to 32M	16M RAM expandable to 32M	16M RAM expandable to 32M
At least 500 MB hard drive	At least 1 GB hard drive	At least 1 GB hard drive
The computer must support user specific requirements for LAN connectivity.	The computer must support user specific requirements for LAN connectivity.	The computer must support user specific requirements for LAN connectivity.
2-PCMCIA type II slots	2-PCMCIA slots	2-PCMCIA slots
SVGA (1024x768 resolution)	SVGA controller with 1MB RAM	SVGA controller with 1MB RAM
	CD-ROM Reader	CD-ROM Reader
	3.5" floppy drive	3.5" floppy drive
	2-parallel and 2-serial ports	2-parallel and 2-serial ports
	3-button mouse	3-button mouse
	17" color monitor	17" color monitor

Table USMC-2 - Minimum USMC Desktop and Server System Requirements

Personal Computer	Server Configuration
Minimum Configuration	
IBM Compatible	Certified for intended Network Operating System
≥ 66MHz Processor Clock Speed	≥ 100 MHz Processor Clock Speed
8 kbytes of Internal Cache	
	Support DX2 Intel Implementation or Better
32-bit Data Path	100% Compatible EISA/PCI Bus
	Four EISA/PCI 32-bit Expansion Board Slots Two EISA/PCI 64-bit Expansion Board Slots One EISA/PCI Shared 64-bit Expansion Board Slots
5 Volt	
EPA Energy Star Compliant	
36 Integer SPECMark	
16 Floating Point SPECMark	
16 Megabytes RAM, Expandable to 32 Megabytes	64 Megabytes of RAM, 70 nS Speed, Extended RAM Memory with the Capability to Increase Total Memory to 128 Megabytes
1 Gigabyte or 2 - 500 Megabyte Hard Drive	Two 1 Gigabyte Hard Drives
2 PCMCIA Type II Slots or 1 Type III	
	One EISA/PCI Fast SCSI II Controller Card or Better
SVGA Controller with 1 Megabyte RAM, 1024x768 Pixels, 256 Colors	
LAN Connectivity	
	Real-time Clock with Battery Backup
3.5-inch Floppy Drive	3.5-inch Floppy Drive
2 Parallel and 2 Serial Ports	
Pointing Device with a Minimum of 2 Buttons	
	1 2/4 Gigabyte 4mm Digital Audio Tape Unit
	EISA/CMOS Configurable to 512k
	Base RAM to Support 5 ICA Cards
14 inch Color Monitor	

USMC 2.1.2.2 Marine Corps Software

Table USMC-3 is a list of the required standard software products by applications category. For individuals performing tasks in one of these application areas, these software packages are those authorized for purchase and use on USMC Personal Computer-Class Systems.

Table USMC-3 - Required Software Products

Software Category	Selected Product
Standard Issue	
Programming Language (Developmental)	Ada
Specialty Items	
Asynchronous Communications	TBD
Audit Software	TBD
Client/Server OS	TBD
Decision Support	TBD
Desktop Publishing	TBD
Disk Management	TBD
Document Management	TBD
Internet Web Browser	TBD
Internet Image Editor	TBD
Message Release	TBD
Network Management Local Management Regional Management	 TBD TBD
Project Management	TBD
SQL Database	Oracle
Voice Recognition	TBD

USMC 2.1.3 Information Transfer Standards

In addition to the TELNET requirements found in Section 3.2.1.1.1.4, Remote Terminal, the following standards are mandated:

- IAB Standard 27/RFC-856, TELNET Binary Transmission
- IAB Standard 28/RFC-857, TELNET Echo Option
- IAB Standard 29/RFC-858, TELNET Suppress Go Ahead Option
- IAB Standard 30/RFC-859, TELNET Status Option
- IAB Standard 31/RFC-860, TELNET Timing Mark Option
- IAB Standard 32/RFC-861, TELNET Extended Options: List Option
- RFC-1041, TELNET 3270 Regime Option.

USMC 2.1.4 Information Modeling and Information Standards

This supplement does not specify any standards in this area.

USMC 2.1.5 Human-Computer Interface

This supplement does not specify any standards in this area.

USMC 2.1.6 Information Systems Security Standards

This supplement does not specify any standards in this area.

USMC 3.1 EMERGING STANDARDS

This supplement does not specify any standards in this area.

Frequently Asked Questions (FAQ) on JTA

1. **What is a technical architecture?** Recent discussions within DoD have defined three types of architectures: operational, technical, and system. The technical architecture is the set of rules, or "building codes", that are used when a system engineer begins to design/specify a system to achieve interoperability. These rules consist primarily of a common set of standards/protocols to be used for sending and receiving information (information transfer standards such as Internet Protocol suite), for understanding the information (information content and format standards such as data elements, or image interpretation standards) and for processing that information. It also includes a common human-computer interface and "rules" for protecting the information (i.e., information system security standards).

2. **What is the Joint Technical Architecture (JTA)?** The JTA is a document that identifies a common set of mandatory information technology standards and guidelines to be used in all Command, Control, Communications, Computers, and Intelligence (C4I) systems and the interfaces of C4I systems with other key assets.

3. **What is C4I in the context of the JTA?** C4I refers to command, control and intelligence systems (to include sustaining base, combat support information systems, and office automation systems) and the communications and computers that directly support them. The JTA also includes the interfaces of those systems with other key assets (e.g., weapon systems, sensors, models and simulations) to support critical joint Warfighter interoperability.

4. **When is the JTA going to be available?** JTA Version 1.0 has been signed out by the Assistant Secretary of Defense (ASD) for Command, Control, Communications, and Intelligence (C3I) (Mr. Paige), the Under Secretary of Defense for Acquisition and Technology (USD(A&T)) (Dr. Kaminski), and the Service Acquisition Executives.

5. **Why is a JTA needed?** The need for better interoperability and information flow across DoD in support of the joint Warfighter has been widely recognized. In order for systems to interoperate in a joint environment, they need to be born joint. The JTA is a key piece of DoD's overall architecture strategy to achieve that goal.

6. **What is the scope of the JTA?** The scope of this initial version of the JTA is focused on C4I systems and the interfaces of those systems with other key assets (e.g., weapon systems, sensors, and models and simulations) to support critical joint Warfighter needs. Future versions of the JTA will extend the Version 1.0 scope from C4I Systems into these other domains.

7. **Who will use the JTA and for what?** The JTA shall be used by anyone involved in the management, development, or acquisition of new or improved C4I systems within DoD. Specific guidance for implementing this JTA is provided separately. System developers shall use the JTA to ensure that new and upgraded C4I systems (and the interfaces to such systems) meet interoperability requirements. System integrators shall use it to facilitate the integration of existing and new systems. Operational requirements developers shall be cognizant of the JTA in developing requirements and functional descriptions. When developing C4I applications for Advanced Technology Demonstrations (ATDs), the science and technology community should use the JTA whenever possible to provide the logical interfaces to existing C4I, so that their good ideas will readily integrate into existing systems rather than require massive redesign to meet DoD's interoperability objectives. The JTA is applicable to Advanced Concept Technology Demonstrations (ACTDs).

8. **Who developed the JTA?** A JTA Working Group (JTA WG) containing the senior technical architects (or their representatives) from each of the Services, ASD(C3I), DIA, DISA (to include DII COE developers), the ISS (representing the broad Intelligence Community), the Joint Staff and the USD(A&T)/Open Systems Joint Task Force, directed the development of the JTA. The actual development was led by DISA with strong Service and Agency participation and used the existing DoD information technology standards structure.

9. **How was the JTA developed?** Strong emphasis was placed on mandating only what was needed, implementable and effective. Focus was on using commercial standards, particularly where products from multiple vendors exist. The first draft of the JTA was widely disseminated (available on the Internet to anyone) for comments in mid-March, second draft end of April. See Section 1.1.8 (Basis for the JTA) for more details.

10. **How does the JTA relate to the COE and TAFIM?** TAFIM provides general guidance and documents the processes and framework for defining the JTA (and other technical architectures). The TAFIM applies to many DoD mission/domain areas and lists all adopted information technology standards that promote interoperability, portability, and scalability. The JTA currently focuses on C4I requirements as related to interoperability by identifying the minimum set of standards for service areas (one standard per function where possible). For the C4I service areas domain, the JTA set of standards supersedes those listed in the TAFIM. The TAFIM Volume 7 should be used as guidance for standards in areas not addressed by the JTA. As the JTA scope expands, the nature and relationship to the standards information in the TAFIM (particularly Volume 7) will evolve. The DII COE is a specific implementation of the technical architecture. See Section 2.1.3 and 2.2 for more details.

11. **What was done to ensure that the JTA will be useful to its stakeholders?** The JTA development process emphasized "user" participation (i.e., PM/developers) as well as the technical standards experts from all of the user communities. Each Service/Agency established continuous communication with their development community and involved them in the standards selection process throughout the development of the JTA. In addition, two drafts have been made available on a public comment basis and a PM Focus Group session was conducted to solicit user community comments. The JTA WG members provide the broad perspective needed to balance requirements and ensure their organization is appropriately represented in its development. Key senior level stakeholders (e.g., the acquisition community) within DoD have been kept informed during the development and progress of the JTA.

12. **What are the implementation plans and strategies for the JTA? How will it be enforced? Will waivers be required? If so, what is the process?** Implementation guidance is contained in the implementation memo signed by the USD (A&T), ASD (C3I) on 22 August 1996 and attached to the JTA Version 1.0. The services and agencies are responsible for the implementation of the JTA (including enforcement) budgeting and determining the pace of systems upgrade. While the strategy is being formulated and discussed now for that guidance, the guiding principle generally agreed to is that the responsibility for specific implementation details, enforcement decisions and mechanisms will be determined by each of the Services and Agencies acquisition executives.

13. **Which systems does it apply to? Does it apply to existing systems? If it does, how quickly will existing systems need to comply?** All emerging C4I systems and C4I systems upgrades are to comply with the JTA. Existing C4I systems are to migrate to the applicable JTA standards, while considering cost, schedule and performance impacts. The Services, Agencies

and other Components are responsible for the implementation of the JTA (including enforcement, budgeting and determining the pace of systems updrades).

14. **Does the JTA apply to leased services?** Yes, at a minimum the JTA standards apply at the interfaces.

15. **Will the JTA be updated? If so, what is the process?** Yes, the JTA must be a "living" document. The JTA must evolve with time as technology and the marketplace changes. In addition, it is intended that the scope of the JTA will expand to include other domains. However, the specifics of the evolution and configuration management process is currently under development.

16. **Why does the JTA have so many standards?** There is a wide range of information systems with many possible interfaces, services and technologies. The JTA currently focuses on C4I requirements as related to interoperability by identifying the minimum set of standards for service areas (one standard per function where possible). To ensure interoperability, the standard for each joint interface must be identified. Generally, a given C4I system will only implement a subset of the functionality defined and therefore need only a subset of the standards from the JTA. Standards in the JTA are "mandatory" in the sense that if a service is going to be implemented, then it must be implemented in accordance with the JTA standards. For example, if your system is not using SATCOM there is no need to implement any of the SATCOM standards. However, if you are implementing a SATCOM capability these standards must be defined for interoperability.

17. **Doesn't the use of standards conflict with DoD's acquisition reform efforts, particularly the use of military standards?** NO!!! The standards and specifications and other standardization documents identified in the JTA are entirely consistent with and support the DoD Standards and Acquisition Reform initiatives. The DoD standards policy recognizes the need for DoD to specify interface standards that are required for interoperability. The standards in the JTA are almost entirely performance-based interface standards. Most are commercial standards. None of the military standards require a waiver to use. A fuller discussion of this is found in Section 1.1.7 and Appendix C.

18. **When a standard identified in the JTA has a new version published, should we assume that the new version is mandated by the JTA?** No! A revised standard is not necessarily backward compatible with the standard it replaces. If the revised standard is backward compatible then it may be considered for use. As a general rule, when newer versions are judged to be mature, with sufficient product support and a clear migration path from the older version is identified (to account for interoperability), they will be mandated in the JTA.

19. **Why are some needed standards such as (TADILs) A, B, C not in the JTA?** The JTA is a forward looking document, defining the standards to which we want to build new systems. The intent is to clearly indicate migration direction. Therefore standards such as these TADILs were viewed as legacy standards and not included.

20. **What do I do when I need standards not listed in the JTA to interface with non-U.S. systems?** In some cases, the citation of JTA standards, for example those for ISDN and SONET, do not assure interoperability in regions outside North America where standards for these services differ. The JTA recognizes that this is a critical area affecting interoperability but does not recommend specific solutions in this version. The system acquisition agency is responsible for analyzing the requirements and choosing appropriate solutions.